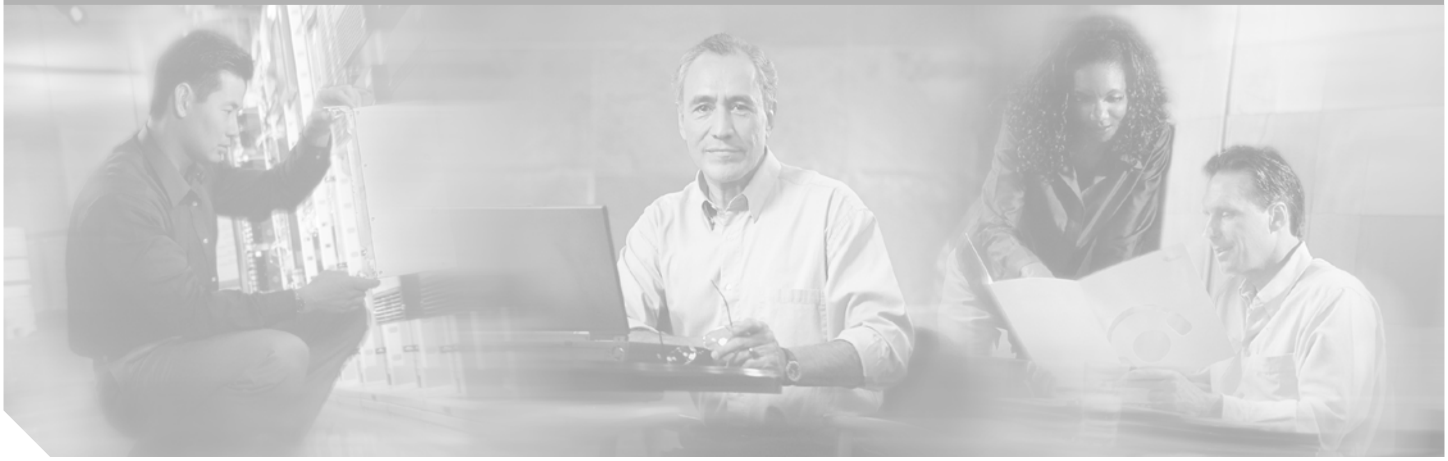


Cisco ONS 15530 Configuration Guide and Command Reference

Cisco IOS Release 12.1(10)EV2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7814227=
Text Part Number: 78-14227-01

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco ONS 15530 Configuration Guide and Command Reference

CONTENTS

CHAPTER 10

Preface

This preface describes the audience, organization, and conventions for the *Cisco ONS 15530 Configuration Guide and Command Reference*, and provides information on how to obtain related documentation.

Audience

This publication is intended for experienced network administrators who are responsible for configuring and maintaining the Cisco ONS 15530.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Product Overview	Provides an overview of the Cisco ONS 15530 features and functions.
Chapter 2	Before You Begin	Describes basic information about the Cisco ONS 15530 CLI interface, IOS mode and naming conventions.
Chapter 3	Initial Configuration	Describes the initial configuration of the Cisco ONS 15530.
Chapter 4	Configuring ESCON Signal Aggregation	Describes how to configure ESCON interfaces and patch connections.
Chapter 5	Configuring Transponder Line Card Interfaces	Describes how to configure transponder interfaces and patch connections.
Chapter 6	Configuring VOA Module Interfaces	Describes how to configure PB-OE modules and WB-VOA modules for signal attenuation.
Chapter 7	Configuring APS	Describes how to configure signal protection on Cisco ONS 15530 systems and networks.
Chapter 8	Configuring Multiple Shelf Nodes	Describes how to configure a network node with multiple Cisco ONS 15530 shelves supporting more than four channels with line card protection.

Chapter	Title	Description
Chapter 9	Monitoring Your Network Topology	Describes how to monitor the operation of Cisco ONS 15530 networks.
Chapter 10	Managing Your Cisco ONS 15530 System	Describes how to manage Cisco ONS 15530 systems.
Appendix A	Command Reference	Lists and describes Cisco ONS 15530 commands.

Related Documentation

This document provides detailed configuration examples for the Cisco ONS 15530; however, it does not provide complete extensive background information on DWDM (dense wavelength division multiplexing) technology or the architecture of the Cisco ONS 15530. For background information on DWDM technology, refer to the *Introduction to DWDM Technology* document.

You will also find useful information on the CLI (command-line interface) and basic shelf management in the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Refer to the following documents for detailed design considerations, hardware installation, safety information, troubleshooting information, and glossary terms:

- *Introduction to DWDM Technology*
- *Cisco ONS 15530 Planning and Design Guide*
- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 series*
- *Cisco ONS 15530 Hardware Installation Guide*
- *Cisco ONS 15530 Alarms and Error Messages*
- *Cisco ONS 15530 MIB Quick Reference*
- *Glossary for Optical Networking Terms*

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Convention	Description
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
→	`This pointer highlights an important line of text in an example.`
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Product Overview

The Cisco ONS 15530 is a highly modular and scalable optical switching and aggregation platform. With the Cisco ONS 15530, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, SAN (storage area network), and TDM (time-division multiplexing) traffic. For more information about DWDM technology and applications, refer to the *Introduction to DWDM Technology* publication and the *Cisco ONS 15530 Planning and Design Guide*.

The Cisco ONS 15530 is designed to meet and exceed the most stringent ISP (Internet service provider) requirements for product availability and reliability. Its features include:

- Redundant fan assemblies
- Redundant power (AC or DC)
- Redundant CPU switch modules
- Interfaces which can be configured for redundancy using SONET 1+1 APS (Automatic Protection Switching)
- Line cards, power supplies, and fan assemblies that are hot-swappable without powering down the shelf

This chapter includes the following sections:

- Cisco ONS 15530 Hardware Features, page 1-1
- Cisco ONS 15530 Software Features, page 1-7

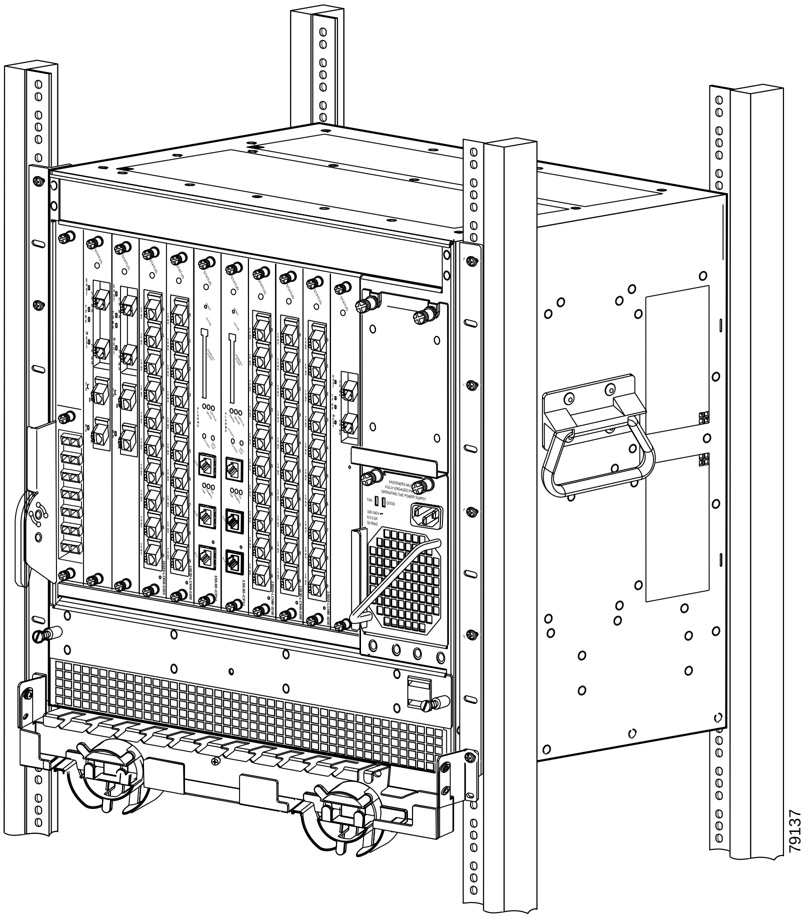
Cisco ONS 15530 Hardware Features

This section describes the hardware features and components of the Cisco ONS 15530.

Chassis Overview

The Cisco ONS 15530 is available in two configurations. Both have two vertically stacked half-height slots specifically for the OADM (optical add/drop multiplexers) modules, and 10 vertically oriented slots which hold the CPU switch modules, line cards, and transponder line cards. As you face the chassis, the leftmost slot (slot 0) holds two half height OADM modules. Slots 1 through 4 and slots 7 through 10 hold the line cards and transponder line cards. Slots 5 and 6 hold the CPU switch modules (see Figure 1-2). Power supplies are located on the right side of the chassis next to slot 10. Air inlet and fan tray are located beneath the slots. Cable management is located above and beneath the slots. The system has an electrical backplane for system control. All optical connections are located on the front of the shelf. The Cisco ONS 15530 supports up to 60 ESCON (Enterprise Systems Connectivity) ports on a single shelf and up to 160 ESCON ports in a stacked shelf solution.

Figure 1-1 Cisco ONS 15530 Shelf



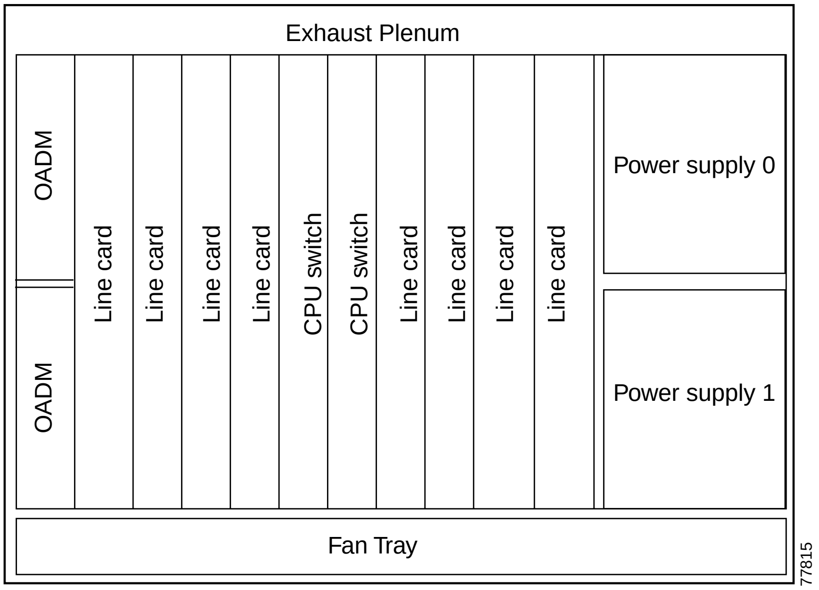
Component Summary

The Cisco ONS 15530 supports the following hot-swappable modular hardware components:

- 10-port ESCON multiplexing line cards, 10-Gbps ITU trunk cards, and 10-GE (Gigabit Ethernet) uplink cards.
- Single-mode and multimode transponder line cards
- OADM (optical add/drop multiplexer) modules
- Carrier motherboards
- OSC (optical supervisory channel) modules
- PB-OE (per-band optical equalizer) modules

- WB-VOA (wide-band variable optical attenuator) modules
- CPU switch modules

Figure 1-2 Cisco ONS 15530 Shelf Layout



ESCON Multiplexing Line Cards, 10-Gbps ITU Trunk Cards, and 10-GE Uplink Cards

The ESCON multiplexing line card aggregates up to 10 client data streams into a single 2.5-Gbps signal. The card sends signal through the switch fabric to a 10-Gbps ITU trunk card or a 10-GE uplink card. The trunk card converts up to four aggregated signals to an ITU-compliant wavelength, or channel. The Cisco ONS 15530 supports two types of 10-Gbps ITU trunk cards:

- Splitter—Sends the channels to two OADM modules.
- Nonsplitter—Sends the channel to only one OADM module.

The 10-Gbps ITU trunk card has an transmit (laser) power in the range of 1 to 5 dBm and a receive detector sensitivity range of –22 to –8 dBm.

The 10-GE uplink card converts up to four aggregated signals to a 10 Gigabit Ethernet 1310-nm signal that can be transmitted to another shelf, such as the Cisco ONS 15540 ESPx and the Cisco ONS 15540 ESP. The transmit power for the 10-GE uplink card is –8.2 to 0.5 dBm and the receive detector range is –14.4 to 0.5 dBm.

For more information on power budget planning, refer to the *Cisco ONS 15530 Planning and Design Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15530 Hardware Installation Guide*.

Transponder Line Cards

The protocol-transparent and bit-rate transparent transponder line card converts a single client signal into an ITU wavelength, or channel.The Cisco ONS 15530 shelf holds up to four transponder line cards, one for each wavelength supported by the OADM modules.

The Cisco ONS 15530 supports four types of single client interface transponder line cards:

- SM (single-mode) nonsplitter
- SM splitter
- MM (multimode) nonsplitter
- MM splitter

Both types of SM transponder line cards accept SM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 2.5 Gbps. Both types of MM transponder line cards accept SM and MM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 622 Mbps.

The transponder line cards are hot pluggable, permitting in-service upgrades and replacement.

All client signals on the transponders are supported in 3R (reshape, retime, retransmit) mode, regardless of protocol encapsulation type. The following protocol encapsulation types are supported in 3R mode plus protocol monitoring:

- ESCON (200 Mbps) SM and MM
- Fibre Channel (1 Gbps) SM
- FICON (Fiber Connection) (800 Mbps) SM
- Gigabit Ethernet (1000 Mbps) SM
- SDH (Synchronous Digital Hierarchy) STM-1 SM and MM
- SDH STM-4 SM and MM
- SDH STM-16 SM
- SONET OC-3 SM and MM
- SONET OC-12 SM and MM
- SONET OC-48 SM
- ISC (InterSystem Channel) links compatibility mode

The following protocol encapsulation types are supported in 3R mode without protocol monitoring:

- Fast Ethernet SM
- FDDI SM
- Fibre Channel (2 Gbps) SM
- ISC peer mode SM
- Sysplex CLO (control link oscillator) MM (8 Mbps)
- Sysplex ETR (external timer reference) MM (8 Mbps)

The client interfaces also support the OFC (open fiber control) safety protocol for Fibre Channel, ISC compatibility mode, and FICON. Client-side interfaces are protocol transparent and can accept signals at specific rates between 16 Mbps and 2.5 Gbps.

On the trunk side, the transponder line card has an output (laser) power in the range of 5 to 10 dBm and a receive detector sensitivity range of –22 to –8 dBm. For more information on power budget planning, refer to the *Cisco ONS 15530 Planning and Design Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15530 Hardware Installation Guide*.

OADM Modules

The Cisco ONS 15530 supports one OADM module in an unprotected configuration or two OADM modules for a protected configuration. Each OADM module can multiplex and demultiplex a band of 4 channels. Channels not filtered by the OADM module are passed on to the next OADM module. In a protected configuration, both OADM modules support the same band of channels to provide fault tolerance.

Carrier Motherboards

The carrier motherboard installs into a single shelf slot and accepts two half-size modules. The carrier motherboard supports the OSC modules and the VOA modules.

OSC Modules

The OSC cards support an optional out-of-band management channel for communicating between systems on the network. Using a 33rd wavelength (channel 0), the OSC allows control and management traffic to be carried without requiring a separate Ethernet connection to each node in the network. Up to two OSC modules can be installed in the carrier motherboard, one card for the west direction and one for the east direction.

The OSC always terminates on a neighboring node. By contrast, data channels may or may not be terminated on a given node, depending on whether the channels on the OADM modules are treated as either express (pass-through) or add/drop channels.

VOA Modules

The Cisco ONS 15530 supports VOA (variable optical attenuator) modules that work with EDFAs (erbium-doped fibre attenuators) to expand DWDM optical networks over greater distances. The VOA modules include PB-OE (per-band optical equalizer) modules and WB-VOA (wide-band variable optical attenuator) modules. These modules are installed in the carrier motherboard.

PB-OE Modules

The PB-OE modules select and attenuate one or two specific 4-channel bands. The Cisco ONS 15530 supports eight single band PBOE modules for bands A through H and four dual band PB-OE modules for bands AB, CD, EF, and GH.

WB-VOA Modules

The WB-VOA modules accept and attenuate an ITU signal regardless of the channels in the signal. This includes signals with a single channel, a band of channels, or multiple bands of channels. There are two types of WB-VOA modules: single and dual. The single WB-VOA module attenuates only one signal and the dual WB-VOA module attenuates up to two signals.

CPU Switch Modules

The Cisco ONS 15530 includes one CPU switch module with a switch fabric. There may be two CPU switch modules in a Cisco ONS 15530 shelf to provide a higher level of system availability. One of the CPU switch modules is the active one (sometimes called primary or master) and the other is the standby (sometimes called secondary, backup, or slave). The standby CPU switch module is present for increased reliability so that it can take over in case the active CPU switch module fails.

Each CPU switch module has a number of subsystems, including a processor, a switch fabric, a clock subsystem, an Ethernet switch for communication between processors and with the LRC (line card redundancy controller) on the OADM modules and line cards, and an SRC (switchcard redundancy controller). The active processor controls the system. All LRCs in the system use the system clock and synchronization signals from the active CPU switch module. Interfaces on the CPU switch modules permit access by 10/100 Ethernet, console terminal, or modem connections.

The key features of the Cisco ONS 15530 CPU switch module are:

- 32 by 32 port non-blocking crosspoint switch fabric with up to 3.125 Gbps per port
- RM7000 64-bit RISC processor with internal cache
- Galileo GT96100 support chip
- Flash SIMM in a socket for up to 32 MB with a default of 16 MB
- Bootflash PROM for up to 512KB
- NVRAM for up to 512KB with time of day clock
- Console and auxiliary serial port with RS-232C interface
- 10/100 MB NME (network management Ethernet) port
- CompactFlash card slot
- System clocking source
- Support for two CPU switch modules
- Operates from 12 V DC from the backplane with on-card generation of 5, 3.3, 2.5 and 1.8 V DC
- Environmental and system monitoring and control
- 9-port Fast Ethernet Switch for communication to line cards
- SRC (switch redundancy controller) for communicating with line cards

Switch Fabric

The switch fabric, which is integrated onto the CPU switch module, is a 36 by 37 crosspoint, nonblocking switch with only 32 by 32 ports used. Each port carries 3.125 Gbps.

The switch fabric has a built-in protection switch that offers less than 10 ms switching time as a standard feature. This allows uniform performance over a wide wavelength range. The built-in optical power output measurement system has a wide dynamic range of –20 dBm to 20 dBm. In addition it offers fast connection setups coupled with lower level adjustment to enable fast network configuration changes.

Cisco ONS 15530 Software Features

The Cisco ONS 15530 offers the following software functionality:

- Cisco IOS software on the CPU switch module.
- Autoconfiguration at startup.
- Autodiscovery of network neighbors.
- Online diagnostics.
- CPU switch module redundancy provided by arbitration of processor status and switchover in case of failure without loss of connections.
- Autosynchronization of startup and running configurations between redundant CPU switch modules.
- Support for in-service software upgrades.
- Support for per-channel APS (Automatic Protection Switching) in point-to-point, ring, and mesh topologies using redundant subsystems that monitor link integrity and signal quality.
- Unidirectional and bidirectional 1+1 path switching.
- System configuration and management through the CLI (command-line interface), accessible through an Ethernet connection or the console terminal.
- Optical power monitoring on the signal from the trunk, digital monitoring on both client and trunk interfaces, and per-channel in-service and out-of-service loopback (client and trunk sides).
- Optional out-of-band management of other Cisco ONS 15530 systems on the network through the OSC (optical supervisory channel).
- In-band management of other Cisco ONS 15530 systems using the in-band message channel.
- Support for network management systems that use SNMP. Its capabilities include configuration management, fault isolation, topology discovery, and path trace.

Network Management Systems

The Cisco ONS 15530 is supported by the following network management systems:

- CiscoView
- CTM (Cisco Transport Manager)

For Embedded CiscoView configuration information, see the "Installing and Configuring Embedded CiscoView" section on page 9-23.

The Cisco ONS 15530 is supported by CTM (Cisco Transport Manager) version 3.1.

For more information on the network management systems that support the Cisco ONS 15530, refer to the *Network Management for the Cisco ONS 15530* document.

Optical Supervisory Channel

The Cisco ONS 15530 supports an optional out-of-band management channel for communicating between systems on the network. Using a 33rd wavelength (channel 0), the OSC allows control and management traffic to be carried without a separate Ethernet connection to each Cisco ONS 15530 in the network. The OSC always terminates on a neighboring node. By contrast, data channels may or may not be terminated on a given node, depending on whether the channels on the OADM modules are treated as either express (pass-through) or add/drop channels.

The OSC carries the following types of information:

- CDP (Cisco Discovery Protocol) packets—Used to discover neighboring devices
- IP packets—Used for SNMP and Telnet sessions between nodes
- OSCP (OSC Protocol) packets—Used to determine whether the OSC link is up using a Hello protocol
- APS protocol packets—Used for controlling signal path switching

Note When the OSC is not present, Cisco ONS 15530 systems can be managed individually by separate Ethernet connections.

The OSC is supported by separate modules and motherboards. The OSC is a full duplex channel that can use a single ring for transmit and receive.

For more information on the OSC and managing Cisco ONS 15530 networks, see Chapter 9, "Monitoring Your Network Topology."

In-Band Message Channel

The in-band message channel establishes a method for providing OAM&P (operations, administration, management, and provisioning) functions in Ethernet packet-based optical networks without a SONET layer or SDH layer. In addition, the in-band message channel enables statistical multiplexing of multiple logical lower-speed signals, such as ESCON signals, within a single optical data channel. The in-band message channel terminates with the data channel, not at each node as does the OSC, thus providing management on a per wavelength basis.

Online Diagnostics

The Cisco ONS 15530 provides the following types of online diagnostic tests:

- Background tests checking system component status and access
- OIR (online insertion and removal) tests for motherboards, cards, and standby processors

Network Topologies

The Cisco ONS 15530 supports the following types of topologies:

- Point-to-point
- Hubbed ring
- Meshed ring

For more information on network topologies, refer to the *Introduction to DWDM Technology* publication and the *Cisco ONS 15540 Planning and Design Guide*.

Standards Compliance

For information on standards compliance for the Cisco ONS 15530, refer to the *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series* publication.

Before You Begin

This chapter provides basic information about the Cisco ONS 15530. This chapter includes the following topics:

- About the CLI, page 2-1
- About Cisco IOS Command Modes, page 2-1
- Interface Naming Conventions, page 2-4
- Configuration Overview, page 2-7

About the CLI

You can configure the Cisco ONS 15530 from the CLI (command-line interface) that runs on the system console or terminal, or by using remote access.

To use the CLI, your terminal must be connected to the Cisco ONS 15530 through the console port or one of the TTY lines. By default, the terminal is configured to a basic configuration, which should work for most terminal sessions.

About Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. To get a list of the commands available in a given mode, type a question mark (?) at the system prompt.

When you start a session on the system, you begin in user mode, also called EXEC mode. Only a limited subset of the commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode. Normally, you must type in a password to access privileged EXEC mode. From privileged mode, you can type in any EXEC command or access global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across system reboots or across processor switchovers.

You can monitor and control the standby processor with commands entered on the active processor. A subset of EXEC and privileged EXEC commands are available through the standby processor console.

Note You can easily determine if you are accessing the active or the standby processor: The standby processor has “sby-” prefixed to the command prompt.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across system reboots. You must start at global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety submodes.

ROM (Read-only memory) monitor mode is a separate mode used when the system cannot boot properly. For example, your system or access server might enter ROM monitor mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted at startup.

Table 2-1 lists and describes the most commonly used modes, how to enter the modes, and the resulting system prompts. The system prompt helps you identify which mode you are in and, therefore, which commands are available to you.

Table 2-1 Frequently Used IOS Command Modes

Mode	Description of Use	How to Access	Prompt
User EXEC	To connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	`Switch>`
Privileged EXEC (Enable)	To set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the **configure** command. Use this command to access the other command modes.	From the user EXEC mode, enter the **enable** command and the enable password.	`Switch#`
Global configuration	To configure features that affect the system as a whole.	From the privileged EXEC mode, enter the **configure terminal** command.	`Switch(config)#`
Interface configuration	To enable features for a particular interface. Interface commands enable or modify the operation of a port.	From global configuration mode, enter the **interface** *type location* command. For example, enter **interface fastethernet 0**	`Switch(config-if)#`
Line configuration	To configure the console port or VTY line from the directly connected console or the virtual terminal used with Telnet.	From global configuration mode, enter the **line console 0** command to configure the console port, or the **line vty** *line-number* command to configure a VTY line.	`Switch(config-line)#`
Redundancy configuration	To configure system redundancy.	From global configuration mode, enter the **redundancy** command.	`Switch(config-red)#`
APS[1] configuration	To configure APS redundancy features.	From redundancy configuration mode, enter the **associate group** command.	`Switch(config-aps)#`

Table 2-1 Frequently Used IOS Command Modes (continued)

Mode	Description of Use	How to Access	Prompt
Threshold list configuration	To configure alarm threshold list attributes and thresholds.	From the global configuration mode, enter the **threshold-list** command.	`Switch(config-t-list)#`
Threshold configuration	To configure alarm threshold attributes.	From threshold list configuration mode, enter the **threshold** command.	`Switch(config-threshold)#`

[1] Automatic Protection Switching

The Cisco IOS command interpreter, called the EXEC, interprets and executes the commands you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **config t**.

When you type **exit**, the CLI backs out one command mode level. In general, typing **exit** returns you to global configuration mode. To exit configuration mode completely and return to privileged EXEC mode, press **Ctrl-Z** or **end**.

Listing Cisco IOS Commands and Syntax

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Switch> ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called word help, because it lists the words for you.

```
Switch# c?
calendar  cd    clear  clock  configure
connect   copy
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Switch# configure ?
  memory             Configure from NV memory
  network            Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal           Configure from the terminal
  <cr>
```

To redisplay a command you previously entered, press the Up-arrow key. You can continue to press the Up-arrow key to see more previously issued commands.

Tips If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

You can press **Ctrl-Z** or **end** in any mode to immediately return to privileged EXEC (enable) mode, instead of entering **exit**, which returns you to the previous mode.

Interface Naming Conventions

This section describes the interfaces and the interface naming conventions for each type of card supported by the Cisco ONS 15530.

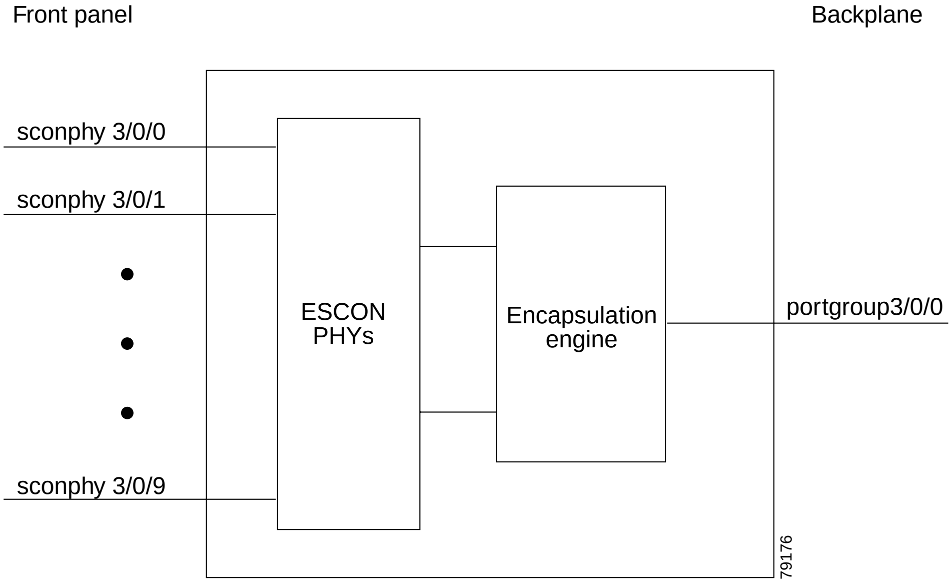
ESCON Multiplexing Line Card Interfaces

The ESCON multiplexing line card has two types of interfaces:

- Esconphy interfaces
- Portgroup interfaces

Figure 2-1 shows the interfaces for the ESCON multiplexing line card.

Figure 2-1 ESCON Multiplexing Line Card Interfaces



Esconphy Interfaces

The esconphy interfaces are located on the front panel of the ESCON multiplexing line cards. Each ESCON multiplexing line card has 10 esconphy interfaces. The ESCON multiplexing line card aggregates the signals from the esconphy interfaces into a single 2.5-Gbps signal and sends it to the portgroup interface on the backplane side of the card. The esconphy is an uncolored interface that carries ESCON physical layer signals. This interface does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the esconphy interfaces on the ESCON multiplexing line card is as follows:

esconphy *slot*/*subcard*/*port*

Portgroup Interfaces

This logical interface represents the aggregation of multiple packet streams from slow speed interfaces. For example, this interface is used on the Cisco ONS 15530 optical switches, where the switching granularity is only on the level of a 2.5-Gbps aggregate packet stream resulting from multiple slow speed interfaces such as esconphy.

The portgroup interfaces are located on the ESCON multiplexing line cards. The portgroup interface connects the esconphy interfaces on the front panel to the switch fabrics. A logical interface representing the aggregation of multiple ESCON client signals.

The naming convention for the portgroup interfaces on the ESCON multiplexing line card is as follows:

portgroup *slot*/*subcard*/*port*

Each ESCON multiplexing line card has only one portgroup interface.

10-Gbps ITU Trunk Card Interfaces

The 10-Gbps ITU trunk cards have four types of interfaces:

- Ethernetdcc interfaces
- Wavethernetphy interfaces
- Wavethernetphy subinterfaces
- Wavepatch interfaces

Figure 2-2 shows the interfaces for the splitter 10-Gbps ITU trunk card. Figure 2-3 shows the interfaces for the nonsplitter 10-Gbps ITU trunk card.

Figure 2-2 Splitter 10-Gbps ITU Trunk Card Interfaces

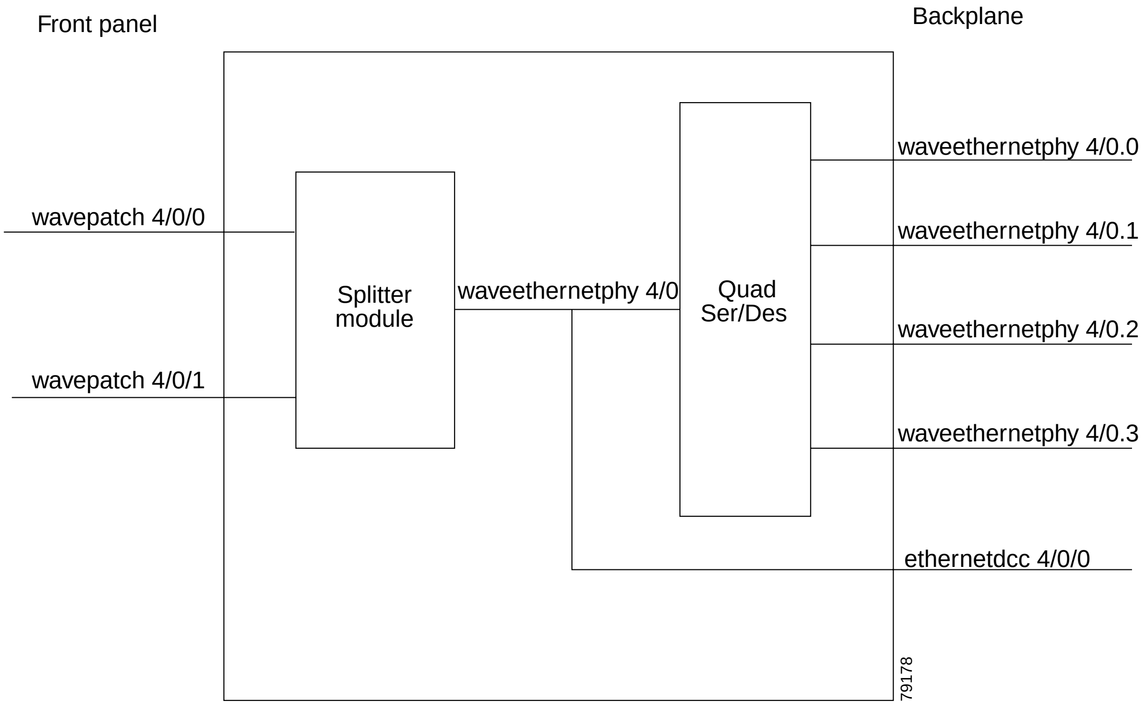
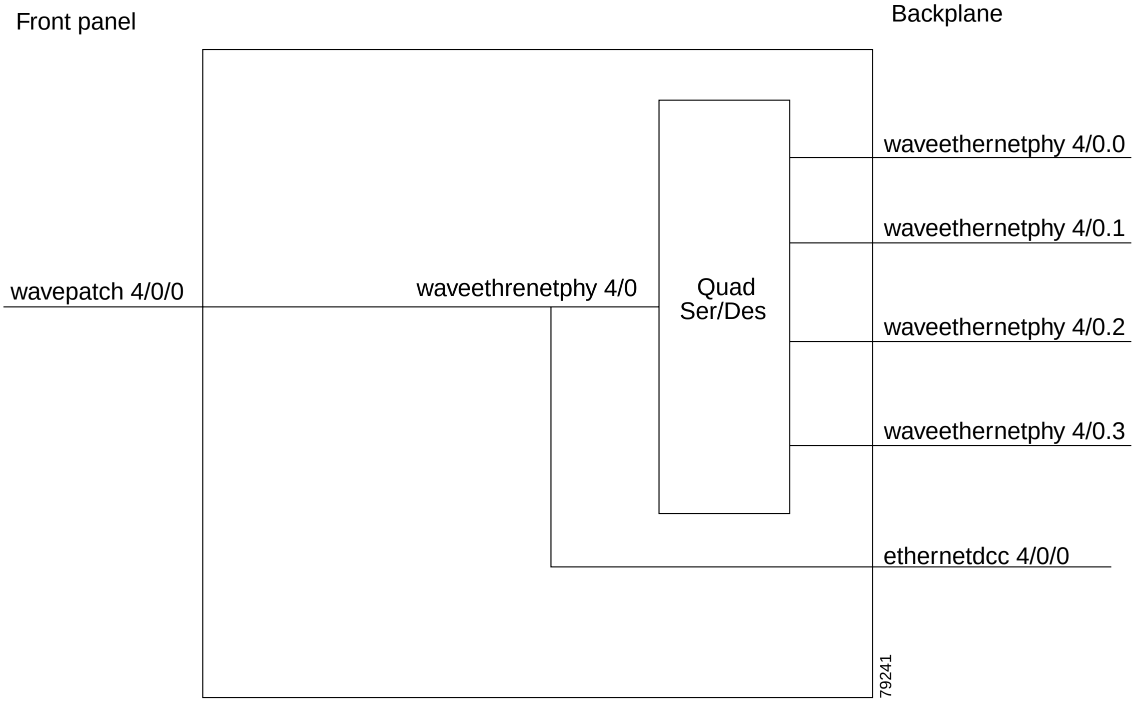


Figure 2-3 Nonsplitter 10-Gbps ITU Trunk Card Interfaces



Ethernetdcc Interfaces

The ethernetdcc interfaces provide the communication path for the in-band message channel OAM messages between the 10-Gbps ITU trunk card and the CPU switch modules. The ethernetdcc interface connects the switch fabrics to the waveethernetphy interface.

The naming convention for ethernetdcc interfaces is as follows:

ethernetdcc *slot*/*subcard*/*port*

Each card has one ethernetdcc interface.

Waveethernetphy Interfaces

The waveethernetphy interfaces correspond to the laser on the 10-Gbps ITU trunk cards.
The waveethernetphy interface connects the four waveethernetphy subinterfaces on the backplane side of the 10-Gbps ITU trunk card to the wavepatch interface on the front panel. The waveethernetphy interface ITU signal carries up to four 2.5-Gbps physical layer signals. It does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the waveethernetphy interfaces is as follows:

waveethernetphy *slot*/*subcard/port*

Each 10-Gbps ITU trunk card has one waveethernetphy interface.

Waveethernetphy Subinterfaces

The waveethernetphy subinterfaces are located on the backplane side of the10-Gbps ITU trunk cards. The waveethernetphy interface connects the switch fabric to the waveethernetphy interface. Each waveethernetphy subinterface can handle 2.5 Gbps of data traffic.

The naming convention for the waveethernetphy subinterfaces is as follows:

waveethernetphy *slot*/*subcard***.***subinterface*

Each 10-Gbps ITU trunk card has four waveethernetphy subinterfaces.

Wavepatch Interfaces

The wavepatch interfaces are on the front panel of the 10-Gbps ITU trunk card. The waveethernetphy interfaces connect to the wavepatch interfaces on the backplane side. The mux/demux filter interfaces connect to the wavepatch interface on the front panel side.

A splitter10-Gbps ITU trunk card has two wavepatch interfaces. An nonsplitter10-Gbps ITU trunk card has only one wavepatch interface.

The wavepatch interface operational state reflects the operational state of the corresponding waveethernetphy interface. If the waveethernetphy interfaces are operationally down, the corresponding wavepatch interfaces are operationally down. Conversely, if the waveethernetphy interfaces are operationally up, then the wavepatch interfaces are up. However, the administrative states of the waveethernetphy and wavepatch interfaces are independently tracked.

The naming convention for wavepatch interfaces is as follows:

wavepatch *slot*/*subcard*/*port*

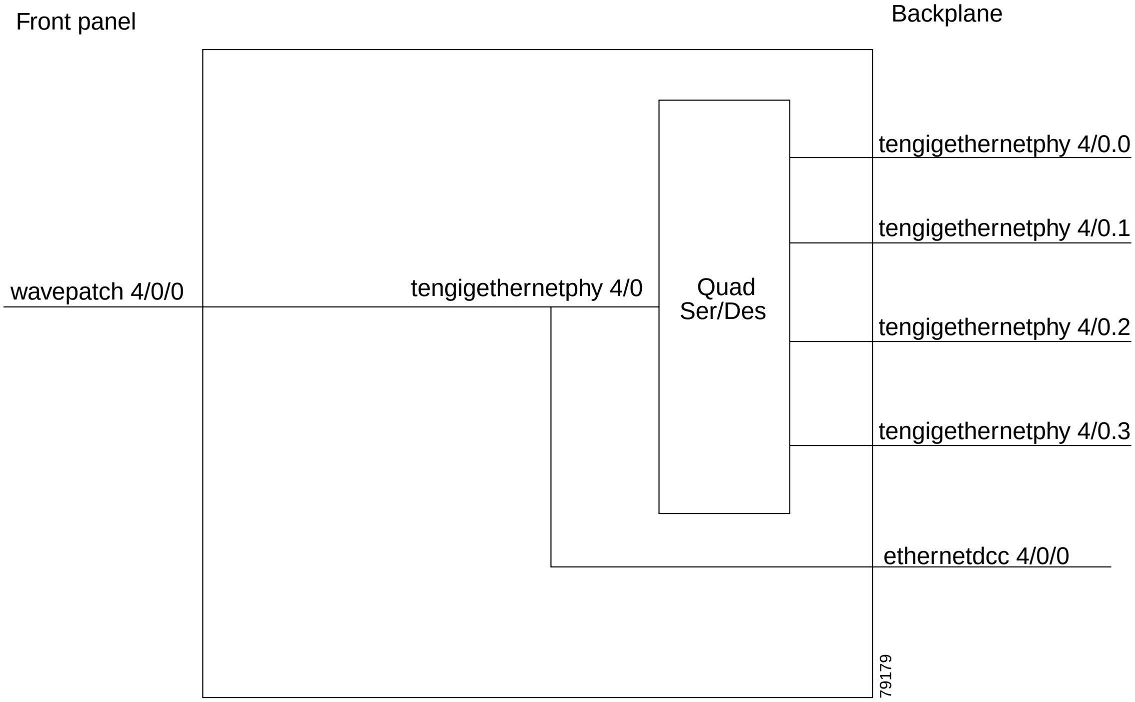
10-GE Uplink Card Interfaces

The 10-GE uplink cards have four types of interfaces:

- Ethernetdcc interfaces
- Tengigethernetphy interfaces
- Tengigethernetphy subinterfaces
- Wavepatch interfaces

Figure 2-4 shows the interfaces for the 10-GE uplink card.

Figure 2-4 10-GE Uplink Card Interfaces



Ethernetdcc Interfaces

The in-band message channel OAM messages for inband management are sent and received by the CPU switch module through the ethernetdcc interfaces. The ethernetdcc interface connects to the switch fabrics on the backplane side and the waveethernetphy interface on the front panel side.

The naming convention for ethernetdcc interfaces is as follows:

ethernetdcc *slot*/*subcard*/*port*

Each 10-GE uplink card has one ethernetdcc interface.

Tengigethernetphy Interfaces

The tengigethernetphy interfaces correspond to the laser on the 10-GE uplink cards. The tengigethernetphy interface connects to the tengigethernetphy subinterface on the backplane side of the 10-GE uplink card and to the wavepatch interface on the front panel side. This is an uncolored interface that carries 10 Gigabit Ethernet. This interface does not terminate layer 2 or layer 3 protocol operations.
The naming convention for the tengigethernetphy interfaces is as follows:
tengigethernetphy *slot*/*subcard/port*

Each 10-GE uplink card has one tengigethernetphy interface.

Tengigethernetphy Subinterfaces

The tengigethernetphy interfaces are the backplane interfaces on the10-GE uplink cards. The tengigethernetphy interface connects to the switch fabric.

The naming convention for the tengigethernetphy subinterfaces is as follows:

tengigethernetphy *slot*/*subcard*.*subinterface*

Each 10-GE uplink card has four tengigethernetphy subinterfaces.

Wavepatch Interfaces

The wavepatch interfaces are on the front panel of the 10-GE uplink card. The tengigethernetphy interfaces connect to the wavepatch interfaces on the backplane side. The client interfaces on other shelves connect to the wavepatch interface on the front panel side.

The wavepatch interface operational state reflects the operational state of the corresponding tengigethernetphy interface. If the tengigethernetphy interfaces are operationally down, the corresponding wavepatch interfaces are operationally down. Conversely, if the tengigethernetphy interfaces are operationally up, then the wavepatch interfaces are up. However, the administrative states of the tengigethernetphy and wavepatch interfaces are independently tracked.

The naming convention for wavepatch interfaces is as follows:

wavepatch *slot*/*subcard*/*port*

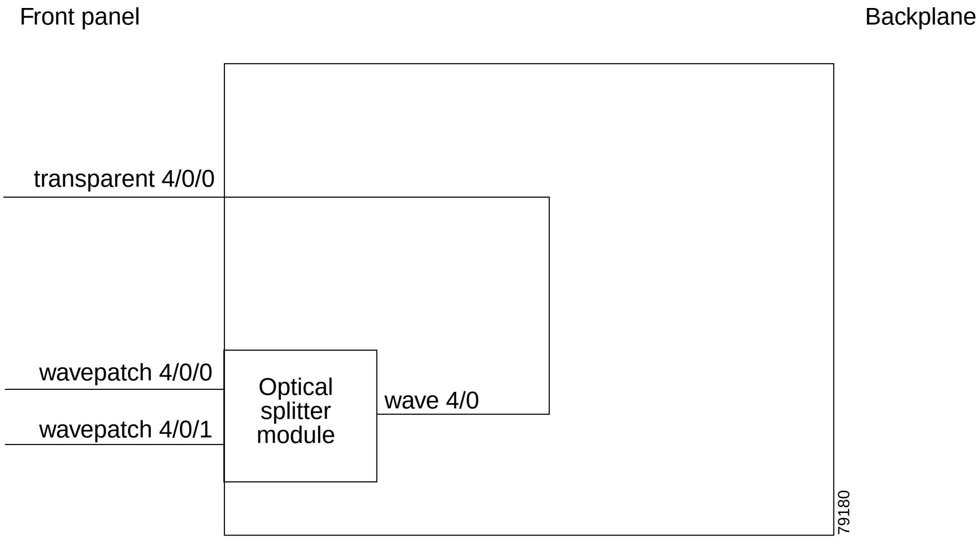
Transponder Line Card Interfaces

The transponder line cards have three types of interfaces:

- Transparent interfaces
- Wave interfaces
- Wavepatch interfaces

Figure 2-5 shows the interfaces for the transponder line card.

Figure 2-5 Transponder Line Card Interfaces



Transparent Interfaces

The transparent interfaces are located on the front panel of the transponder line cards. The interface does not terminate the protocol, hence the term *transparent*. Also, transparent applies to transparency with regard to networking protocols. The transparent interface connects to the wave interface on the backplane side of the transponder line card.

The naming convention for the transparent interfaces is as follows:

transparent *slot*/*subcard*/*port*

Each transponder line card has one transparent interface.

Wave Interfaces

The wave interface corresponds to the laser on the transponder line card that generates the channel. The wave interface electrically connects to the transparent interface on the front panel and optically connects to two wavepatch interfaces on a splitter card, or to one wavepatch interface on a nonsplitter card, on the ITU side.

The naming convention for wave interfaces is as follows:

wave *slot*/*subcard*

Each transponder line card has one wave interface.

Wavepatch Interfaces

The wavepatch interface is the interface on the front panel that connects to the filter interfaces on the OADM modules. The wave interfaces on the backplane side of the transponder line cards connect to the wavepatch interfaces.

Splitter transponder line cards have two wavepatch interfaces. Nonsplitter transponder line cards have only one wavepatch interface.

The wavepatch interface operational state reflects the operational state of the corresponding wave interface. If the wave interfaces are operationally down, the corresponding wavepatch interfaces are operationally down. Conversely, if the wave interfaces are operationally up, then the wavepatch interfaces are up. However, the administrative states of the wave and wavepatch interfaces are independently tracked.

The naming convention for wavepatch interfaces is as follows:

wavepatch *slot*/*subcard*/*port*

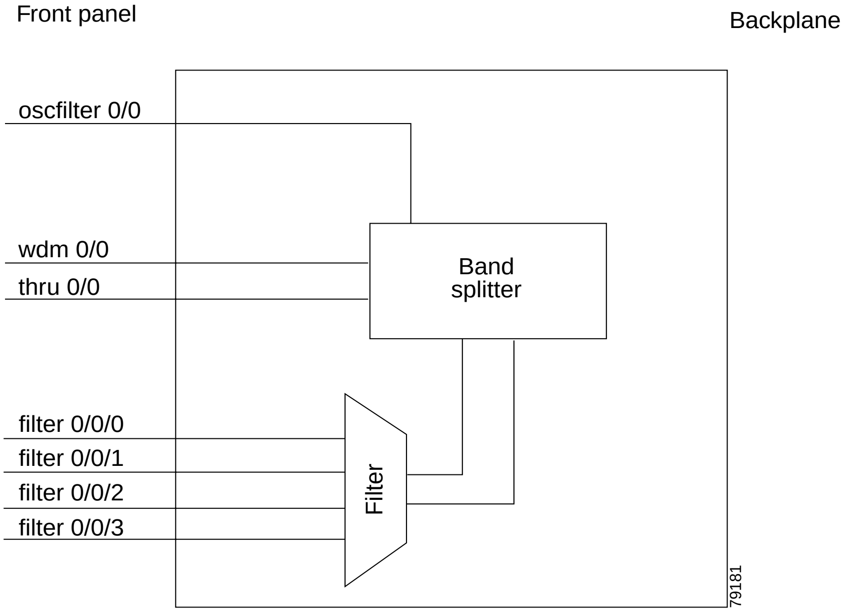
OADM Module Interfaces

The OADM modules can have four types of interfaces:

- Filter interfaces
- Oscfilter interfaces
- Wdm interfaces
- Thru interfaces

Figure 2-6 shows the interfaces for the OADM module.

Figure 2-6 OADM Module Interfaces



Filter Interfaces

The filter interface connects to a wavepatch interface on either a transponder line card or a 10-Gbps ITU trunk card. Each filter interface corresponds to an individual wavelength filter. The filter interface connects a wavepatch interface to a wdm interface on the same OADM module.

The naming convention for filter interfaces is as follows:

filter *slot*/*subcard*/*port*

Each OADM module has four filter interfaces.

Oscfilter Interfaces

The OADM modules can support an optional OSC with an oscfilter interface. This interface connects to the wave interface on an OSC card.

The naming convention for the OSC interface on an OADM module is as follows:

oscfilter *slot*/*subcard*

Wdm Interfaces

The wdm interface is the interface on the OADM module that receives the DWDM signal containing wavelengths to be dropped, or transmits the DWDM signal with added wavelengths. It represent the pairs of fibers (Tx and Rx) on the front panel of an OADM module. The wdm interface connects either to a wdm interface on another network node, or to a thru interface on an OADM module on a different chassis in the same network node.

The naming convention for wdm interfaces is as follows:

wdm *slot*/*subcard*

Thru Interfaces

The thru interface is the interface on the OADM module that sends the DWDM signal to, or receives it from, another OADM module without altering it. It represents the pairs of fibers (Tx and Rx) on the front panel of an OADM module. The thru interface connects to the thru interface on the OADM module in the other subslot on the same chassis, or to a wdm interface on an OADM module on another chassis in the same network node.

The naming convention for thru interfaces is as follows:

thru *slot*/*subcard*

OSC Card Interfaces

The optional OSC provides out-of-band management communications among the Cisco ONS 15530 systems in a network. The OSC is separate from the 32 data channels. The OSC card has one interface, the wave interface.

Wave Interfaces

The wave interface corresponds to the laser on the OSC card that generates the channel. The shelf can have up to two OSCs in the OSC motherboard, one per OADM module.

The naming convention for the OSC interface on an OADM module is as follows:

wave *slot*/*subcard*

CPU Switch Module Interfaces

The CPU switch modules have two types of interfaces:

- NME (network management Ethernet) interfaces
- Auxiliary port interfaces

NME Interfaces

Each CPU switch module has a Fast Ethernet interface, called an NME, for network management purposes. The NME interface on the active CPU switch module is named fastethernet 0 and the NME interface on the standby CPU switch module is named as fastethernet-sby 0.

Each NME interface has a unique MAC address. Also, you must configure each NME interface with a unique IP address. After a processor switchover, when the standby CPU switch module takes over as active, the IP and MAC addresses of the standby CPU switch module are reinitialized to those of the active CPU switch module.

Note Network management system sessions and Telnet sessions are allowed on the NME interface on the active CPU switch module (fastethernet 0) but not allowed on the NME interface on the standby CPU switch module (fastethernet-sby 0).

Auxiliary Port Interfaces

Each CPU switch module has an auxiliary port interface. You can use this interface for modem connections. This interface is named aux 0. The DUART provides two UART channels, both of which connects to an RJ-45 connector on the front panel as the console and auxiliary ports. Typically, the console port connects to a console for configuring, controlling, or debugging the CPU switch module.

WB-VOA Card Interfaces

WB-VOA (wide-band variable optical attenuator) modules have two types of interfaces:

- Voain interfaces
- Voaout interfaces

Voain Interfaces

The voain interface is the input interface on a WB-VOA module. It accepts the signal to be attenuated.

The naming convention for the voain interface on a VOA card is as follows:

voain *slot*/*subcard/port*

Voaout Interfaces

The voaout interface is the output interface on a WB-VOA module. It transmits the attenuated signal.

The naming convention for the voaout interface on a VOA module is as follows:

voaout *slot*/*subcard/port*

PB-OE Module Interfaces

PB-OE (per-band optical equalizer) modules have four types of interfaces:

- Voafilterin interfaces
- Voafilterin subinterfaces
- Voafilterout interfaces
- Voabypassin interfaces
- Voabypassout interfaces

Voafilterin Interfaces

The voafilterin interface identifies the physical port on the PB-OE that accepts the incoming DWDM signal for power equalization.

The naming convention for the voafilterin interface on a PB-OE module is as follows:

voafilterin *slot*/*subcard*/*port*

Voafilterin Subinterfaces

The voafilterin subinterface identifies the attenuator within the PB-OE module.

The naming convention for the voafilterin interface on a PB-OE module is as follows:

voafilterin *slot*/*subcard*/*port***.***subinterface*

Single band PB-OE modules have one voafilterin subinterface. Dual band PB-OE modules have two voafilterin subinterfaces.

Voafilterout Interfaces

The voafilterout interface sends the DWDM signal to the EDFA (erbium-doped fiber amplifier) or the next node in the network topology.

The naming convention for the voafilterout interface on a PB-OE module is as follows:

voafilterout *slot*/*subcard*/*port*

Voabypassout Interfaces

The voabypassout interface carries that portion of the signal not attenuated by the PB-OE module. This interface connects to another VOA module input interface (either a voain interface or a voafilterin interface) where the signal is further attenuated.

The naming convention for the voabypassout interface on a PB-OE module is as follows:

voabypassout *slot*/*subcard*/*port*

Voabypassin Interfaces

The voabypassin interface carries that portion of the signal attenuated on other modules. This interface connects to another VOA module output interface (either a voaout interface or a voafilterout interface) where the signal was attenuated.

The naming convention for the voabypassin interface on a PB-OE module is as follows:

voabypassin *slot*/*subcard*/*port*

Configuration Overview

To configure your Cisco ONS 15530 systems and network, perform the following steps:

Step 1 Select line cards and modules to meet your requirements.

For detailed information about the hardware components, refer to the *Cisco ONS 15530 Hardware Installation Guide*. For detailed information on system planning and design, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Step 2 Insert the cards, motherboards, and CPU switch modules into the chassis.

For detailed information on hardware configuration rules, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Step 3 Configure the NME ports on the active CPU switch module and on the standby CPU switch module, if present.

For detailed information on configuring the NME port, see Chapter 3, "Initial Configuration."

Step 4 Connect the cards with optical cables. Configure the patch connections with the CLI.

For detailed information on cabling between OADM modules, refer to the *Cisco ONS 15530 Planning and Design Guide*. For information on configuring cross connections, see the "Configuring Cross Connections" section on page 4-11.

Step 5 Configure aggregation flow identifier, the cross connections, and the patch connections for all ESCON multiplexing line card and 10-Gbps ITU trunk card interfaces in the shelf. Also, configure the alarm thresholds (optional).

For detailed information on configuring these interfaces, see Chapter 4, "Configuring ESCON Signal Aggregation."

Step 6 Configure either the protocol encapsulation or the clock rate for the client signal for all transponder line cards interfaces in the shelf. Also, enable protocol monitoring for supported protocols and configure the alarms thresholds (optional).

For detailed information on transponder line card interface configuration, see Chapter 5, "Configuring Transponder Line Card Interfaces."

Step 7 Configure the VOA modules (optional).

For detailed information on VOA module interface configuration, see Chapter 6, "Configuring VOA Module Interfaces."

Step 8 Configure APS.

For detailed information on configuring APS, see Chapter 7, "Configuring APS."

Step 9 Configure CPU switch module redundancy.

For detailed information on CPU switch module redundancy, see the "About CPU Switch Module Redundancy" section on page 3-8.

Step 10 Configure IP connectivity on the OSC or through the in-band message channel for network management.

For detailed information on configuring IP connectivity on the OSC, see the "Configuring IP on the OSC" section on page 9-9. For information on configuring IP connectivity via the in-band message channel, see the "Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel" section on page 9-12.

Step 11 Configure CDP and the network topology.

For detailed information on network monitoring, see Chapter 9, “Monitoring Your Network Topology.”

Initial Configuration

This chapter describes how to configure the Cisco ONS 15530 so it can be accessed by other devices.

About the CPU Switch Module

The CPU switch module provides intelligence to the Cisco ONS 15530. The CPU switch module supports SNMP (Simple Network Management Protocol) and many MIBs (Management Information Bases).

The Cisco ONS 15530 uses a QED RM7000 RISC processor. It runs at 78 MHz externally and at 234 MHz internally. It has a 64-bit multiplexed address and data bus with byte parity running at 78 MHz. It has separate internal L1 instruction and data caches of 16 KB each and internal L2 combined instruction/data cache of 256 KB.

The CPU switch modules also contains a 32 by 32 switch fabric that directs traffic from client cards to trunk cards. The switch fabric supports 2.5 Gbps data signals with 2R transparency.

The CPU switch module provides a slot on the front panel that accommodates a CompactFlash card. You can use the CompactFlash card for system image upgrades, FPGA image upgrades, statistics gathering, and other file system applications.

The Cisco ONS 15530 supports redundant operation with dual CPU switch modules. The CPU switch modules reside in slots 5 and 6, the sixth and seventh slots from the left as you face the chassis. For more information about redundancy, see the "About CPU Switch Module Redundancy" section on page 3-8.

For more information on the CPU switch module, refer to the *Cisco ONS 15530 ESP Hardware Installation Guide*.

Starting Up the Cisco ONS 15530

Before starting up the Cisco ONS 15530, you should verify the following:

- The system is set for the correct AC (or DC) power voltages.

  Refer to the *Cisco ONS 15530 Hardware Installation Guide* for correct power voltages.
- The cables are connected to the system.
- A console terminal is connected to the system.

  Refer to the *Cisco ONS 15530 Hardware Installation Guide* for instructions.

When you start up the Cisco ONS 15530, the CLI (command-line interface) prompts you to enter the initial configuration dialog. Answer **no** to this prompt:

```
Would you like to enter the initial dialog? [yes]: no
```

You see the following user EXEC prompt:

```
Switch>
```

You can now begin configuring the CPU switch module.

Using the Console Ports, NME Ports, and Auxiliary Ports

You can configure the Cisco ONS 15530 from a direct console connection to the console port or remotely through its NME (network management Ethernet) port.

- If you are using a direct console connection, configure your terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.
- If you are using the NME port interface, you must assign an IP address to the interface (fastethernet 0).

  For interface configuration instructions, see the "Configuring IP Access on the NME Interface" section on page 3-3.

For further details on configuring ports and lines for management access, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Modem Support

The auxiliary port of the Cisco ONS 15530 provides modem connection support. The following settings on the modem are required:

- Enable auto answer mode.
- Suppress result codes.
- Ensure auxiliary port terminal characteristics, such as speed, stop bits, and parity, match those of the modem.

You can configure your modem by setting the DIP switches on the modem itself or by setting them through terminal equipment connected to the modem. Refer to the user manual provided with your modem for the correct configuration information.

For further details on configuring ports and modems for management access, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Dial Services Configuration Guide: Terminal Services*.

About Passwords

You can configure both an enable password and an enable secret password. For maximum security, the enable password should be different from the enable secret password.

Enable Password

The enable password is a nonencrypted password that controls access to various commands and configuration modes. It contains from 1 to 25 uppercase and lowercase alphanumeric characters. Give the enable password only to users permitted to make configuration changes to the Cisco ONS 15530.

Enable Secret Password

The enable secret password is a secure, encrypted password. On systems running Cisco IOS, you must type in the enable secret password before you can access global configuration mode.You must type in the enable secret password to access boot ROM software.

⚠ **Caution** If you specify an encryption-type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

An enable secret password contains from 1 to 25 uppercase and lowercase alphanumeric characters. The first character cannot be a number. Spaces are valid password characters. Leading spaces are ignored; trailing spaces are recognized.

You will configure passwords in the next section, Configuring IP Access on the NME Interface.

Configuring IP Access on the NME Interface

The Fast Ethernet interface, or NME, on the active CPU switch module, named *fastethernet 0*, is the management interface that allows multiple, simultaneous Telnet or SNMP network management sessions.

You can remotely configure the Cisco ONS 15530 through the Fast Ethernet interface, but first you must configure an IP address so that the active CPU switch module is reachable. You can configure the NME interface two ways: manually from the CLI or by copying the configuration from the BOOTP server into NVRAM.

For information on configuring the NME interface on the standby CPU switch module, *fastethernet-sby 0*, see the "Booting from a TFTP Server" section on page 10-7.

Note Before you begin to manually configure an NME interface, obtain its IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

To configure IP access on the NME port fastethernet 0 from the CLI, perform these steps from the console interface:

	Command	Purpose
Step 1	Switch> **enable** Switch#	Enters privileged EXEC mode.
Step 2	Switch# **show hardware**	Verifies the installed hardware part numbers and serial numbers.
Step 3	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 4	Switch(config)# **enable password** *password*	Sets the enable password. See the "About Passwords" section on page 3-3.
Step 5	Switch(config)# **enable secret** *password*	Specifies an enable secret password. Once set, the enable secret password must be entered to gain access to global configuration mode.
Step 6	Switch(config)# **interface fastethernet 0** Switch(config-if)#	Enters interface configuration mode on interface fastethernet 0, the NME port on the active CPU switch module.
Step 7	Switch(config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and IP subnet mask for the management port interface.
Step 8	Switch(config-if)# **speed** {**10** | **100** | **auto**}	Specifies the transmission speed. The default is **auto** (autonegotiation).
Step 9	Switch(config-if)# **duplex** {**auto** | **full** | **half**}	Specifies the duplex mode. The default is **auto** (autonegotiation).
Step 10	Switch(config-if)# **exit** Switch(config)#	Returns to global configuration mode.
Step 11	Switch(config)# **line vty** *line-number* Switch(config-line)#	Enters line configuration mode for virtual terminal connections. Commands entered in this mode control the operation of Telnet sessions.
Step 12	Switch(config-line)# **password** *password*	Specifies a password for Telnet sessions.
Step 13	Switch(config-line)# **end** Switch#	Returns to privileged EXEC mode.
Step 14	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration changes to NVRAM.

The Cisco ONS 15530 NME interface should now be operating correctly.

Note If a CPU switch module switchover occurs, you can use the same IP address to access the redundant CPU switch module after it becomes active.

Note In a multiple shelf node configuration, perform these steps on the NME interfaces on all shelves in the node.

Displaying the NME Interface Configuration

To display the configuration of the NME interface, use the following EXEC command:

Command	Purpose
show interfaces fastethernet 0	Displays the NTP status.

Example

```
Switch# show interfaces fastethernet 0
FastEthernet0 is up, line protocol is up
  Hardware is AmdFE, address is 0000.1644.28ea (bia 0000.1644.28ea)
➔ Internet address is 172.20.54.152/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
➔ Half-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 3000 bits/sec, 6 packets/sec
  5 minute output rate 1000 bits/sec, 3 packets/sec
     36263 packets input, 3428728 bytes
     Received 17979 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     20363 packets output, 4279598 bytes, 0 underruns
     0 output errors, 8 collisions, 0 interface resets
     0 babbles, 0 late collision, 72 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Displaying the Operating Configurations

You can display the configuration file when you are in privileged EXEC (enable) mode.

- To see the current operating configuration, enter the following command at the enable prompt:

  ```
  Switch# more system:running-config
  ```

- To see the configuration saved in NVRAM, enter the following command:

  ```
  Switch# more nvram:startup-config
  ```

If you made changes to the configuration, but did not yet write the changes to NVRAM, the contents of the running-config file will differ from the contents of the startup-config file.

Configuring the Host Name

In addition to passwords and an IP address, your initial configuration should include the host name to make it easier to configure and troubleshoot the Cisco ONS 15530. To configure the host name, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# **hostname** *name*	Specifies a system name.
Step 3	*name*(config)# **end** *name*#	Returns to privileged EXEC mode. The prompt indicates that the host name has been set to the new name.
Step 4	*name*# **copy system:running-config nvram:startup-config**	Saves your configuration changes to NVRAM.

Note The host name is also synchronized with the standby CPU switch module. The host name prompt on the standby CPU switch module appears with "sby-" as a prefix.

Example

The following example shows how to configure a new host name, beginning in privileged EXEC mode:

```
Switch# configure terminal
Switch(config)# hostname ONS15530
ONS15530(config)# end
ONS15530# copy system:running-config nvram:startup-config
```

About NTP

The NTP (Network Time Protocol) is a utility for synchronizing system clocks over the network, providing a precise time base for networked workstations and servers. In the NTP model, a hierarchy of primary and secondary servers pass timekeeping information by way of the Internet to cross-check clocks and correct errors arising from equipment or propagation failures.

An NTP server must be accessible by the client switch. NTP runs over UDP (User Datagram Protocol), which in turn runs over IP. NTP is documented in RFC 1305. All NTP communication uses UTC (Coordinated Universal Time), which is the same as Greenwich Mean Time. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

- NTP never synchronizes to a machine that is not synchronized itself.
- NTP compares the time reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of machines with an association.

The Cisco implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that you obtain the time service for your network from the public NTP servers available in the IP Internet. If the network is isolated from the Internet, the Cisco NTP implementation allows a machine to be configured so that it acts as though it is synchronized using NTP, when in fact it has determined the time using other means. Other machines then synchronize to that machine using NTP.

A number of manufacturers include NTP software for their host systems, and a version for systems running UNIX and its various derivatives is also publicly available. This software allows host systems to be time-synchronized as well.

Configuring NTP

NTP services are enabled on all interfaces by default. You can configure your Cisco ONS 15530 in either of the following NTP associations:

- Peer association—This system either synchronizes to the other system or allows the other system to synchronize to it.
- Server association—This system synchronizes to the other system, and not the other way around.

From global configuration mode, use the following procedure to configure NTP in a server association that transmits broadcast packets and periodically updates the calendar:

	Command	Purpose
Step 1	Switch(config)# **ntp update-calendar**	Updates hardware calendar with NTP time.
Step 2	Switch(config)# **ntp server** *ip-address*	Forms a server association with another system. You can specify multiple associations.
Step 3	Switch(config)# **end** Switch#	Returns to privileged EXEC mode.
Step 4	Switch# **copy system:running-config nvram:startup-config**	Saves your configuration changes to NVRAM.

For information on other optional NTP configurations, see the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Displaying the NTP Configuration

To view the current NTP configuration and status, use the following EXEC command:

Command	Purpose
show ntp status	Displays the NTP status.

Example

The following example shows the NTP configuration and status:

```
Switch# show ntp status
Clock is synchronized, stratum 4, reference is 198.92.30.32
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is B6C04F19.41018C62 (18:21:13.253 UTC Thu Feb 27 1997)
clock offset is 7.7674 msec, root delay is 113.39 msec
root dispersion is 386.72 msec, peer dispersion is 1.57 msec
```

About CPU Switch Module Redundancy

The Cisco ONS 15530 supports fault tolerance by allowing the standby CPU switch module to take over if the active CPU switch module fails. This standby, or redundant, CPU switch module runs in hot-standby state. In hot-standby state, the standby CPU switch module is partially booted with Cisco IOS software, but no configuration is loaded.

At the time of a switchover from the active CPU switch module, the standby CPU switch module becomes active and loads the configuration as follows:

- If the running configuration file on the active and standby CPU switch modules match, the new active CPU switch module uses the running configuration file.
- If the running configuration file on the new active CPU switch module is missing or invalid, the new active CPU switch module uses the startup configuration file in its NVRAM (not the NVRAM of the former active CPU switch module).

The former active CPU switch module then reloads and becomes the standby CPU switch module.

Note If the standby CPU switch module is unavailable, the system reports a minor alarm. Use the **show facility-alarm status** command to display the redundancy alarm status.

When the Cisco ONS 15530 is powered on, the two CPU switch modules arbitrate to determine which is the active CPU switch module and which is the standby CPU switch module. The following rules apply during arbitration:

- A newly inserted CPU switch module always comes up as the standby CPU switch module, except in cases where the newly inserted card is the only one present.
- If one of the CPU switch modules cannot boot its software image, the redundant CPU switch module boots as the active CPU switch module, allowing you to correct the situation manually.
- The primary route processor at the time the system is powered off continues as the primary when the system is powered on.
- If none of the above conditions is true, the CPU switch module in slot 6 becomes the active CPU switch module.

During normal operation, the active CPU switch module boots completely. The standby CPU switch module partially boots, stopping short of parsing the configuration. From this point, the active and standby CPU switch modules communicate periodically to synchronize any system configuration changes.

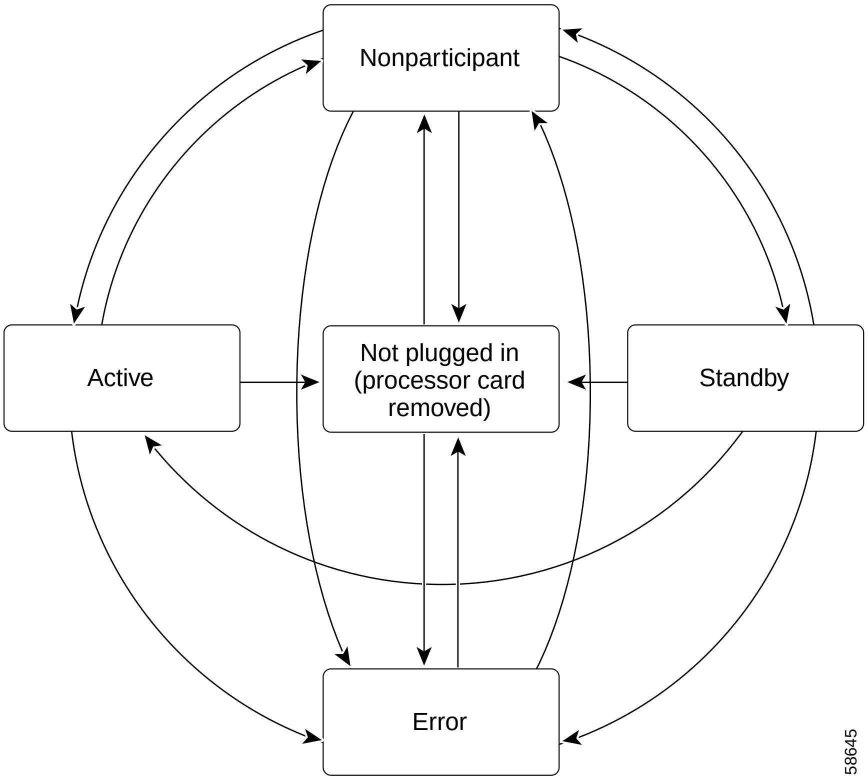
Table 3-1 describes the five CPU switch module hardware states.

Table 3-1 CPU Switch Module Hardware States

State	Description
Active	Processor card is currently providing clock signals and control for all system cards. The active CPU switch module responds to the configured management IP address.
Standby	Processor card is partially booted in hot-standby state waiting to switch over when the active CPU switch module fails, when it is rebooted or removed, or when a manual switchover is requested.
Nonparticipant	Processor card is in ROMMON mode, or is in the process of booting, or has not yet reached the hot-standby state. Manual switchovers are rejected unless the force option is used.
Not plugged in	Processor card slot is empty.
Error	Processor card is present but either the interprocess arbitration interface is not functioning or the CPU switch module is not fully seated in the chassis slot.

Figure 3-1 shows the valid hardware transition states for a system with redundant CPU switch modules.

Figure 3-1 CPU Switch Module State Transition Diagram



In response to redundancy events, such as switchovers and reboots of the active CPU switch module, the software transitions through a series of software redundancy states. Table 3-2 lists some of the significant software states.

Table 3-2 CPU Switch Module Software States

State	Description
Disabled	The standby CPU switch module is not yet running the system image or is in maintenance mode.
Standby cold	The standby CPU switch module is running the system image but has not begun to synchronize data from the active CPU switch module.
Standby hot	The standby CPU switch module has fully synchronized the configuration and other data from the active CPU switch module. It will remain in the hot-standby state until a switchover occurs.
Active	The CPU switch module is in the active hardware state and has completed all switchover or initial bootup processing. It is fully ready to control the system.

Redundant Operation Requirements

For fully redundant operation, the following requirements must be met:

- Two CPU switch modules are required.
- The CPU switch modules must have identical hardware configurations. This includes variables such as DRAM size, and so on.
- Both CPU switch modules must have the same functional image.
- Both CPU switch modules must be running compatible system images. System images are compatible across one major release.
- Both the running and startup configurations are automatically synchronized between the CPU switch modules.
- Both CPU switch modules must be set to autoboot (a default setting).

If these requirements are met, the Cisco ONS 15530 runs in redundant mode by default. If they are not met, the system is conditionally redundant.

Note For detailed information on updating system images, see the "Updating System Images on Redundant Processors" section on page 10-14.

Conditions Causing a Switchover from the Active CPU Switch Module

The following conditions can cause a switchover from the active CPU switch module to the standby CPU switch module:

- The active CPU switch module is removed or swapped. When the CPU switch module functioning as the active CPU switch module is removed, the standby CPU switch module takes over. The Cisco ONS 15530 is nonredundant until a second CPU switch module is inserted.
- The active CPU switch module is rebooted. When a CPU switch module functioning as the active CPU switch module is rebooted, it relinquishes its active role if the standby CPU switch module has reached the hot-standby state.
- The active CPU switch module fails. The standby CPU switch module takes over as the active CPU switch module, using the last synchronized running configuration file (or the last saved startup configuration file if the running configuration file synchronization was disabled or failed).
- A switchover is manually forced with the **redundancy switch-activity** command.

Configuring CPU Switch Module Redundancy

This section describes how to configure CPU switch module redundancy for your Cisco ONS 15530.

Note The initial default configuration will support CPU switch module redundancy and database synchronization with no manual configuration required.

Forcing a Switchover from Privileged EXEC Mode

You can manually force the standby CPU switch module to take over as the active CPU switch module from privileged EXEC mode. To force a switchover from privileged EXEC mode, enter the following command on the active CPU switch module CLI:

Command	Purpose
redundancy switch-activity [**force**]	Causes a CPU switch module switchover. If the standby CPU switch module has not reached the hot-standby software state, use the **force** option.

As long as you have not changed the default configuration register setting from autoboot, the standby CPU switch module (formerly the active CPU switch module) automatically boots until it reaches the hot-standby state.

Note Data transmission through the system is not affected by a CPU switch module switchover.

Example

The following example shows how to manually cause a CPU switch module switchover from privileged EXEC mode:

```
Switch# redundancy switch-activity
This will reload the active unit and force a switch of activity [confirm] y
Preparing to switch activity

00:12:05: %SYS-5-RELOAD: Reload requested
<Information deleted>
```

Forcing a Switchover from ROM Monitor Mode

You can manually force the standby CPU switch module to take over as the active CPU switch module ROM monitor mode. To force a switchover from ROM monitor mode, enter the following commands on the active CPU switch module CLI:

Command	Purpose
switchover	Causes a CPU switch module reset and switchover. The CPU switch module stays in ROM monitor mode.

Note Using the **reset** command in ROM monitor mode on the active processor CLI under normal conditions does not cause a switchover.

Example

The following example shows how to manually cause a CPU switch module switchover from ROM monitor mode:

```
<Information deleted>

→ This CPU is ACTIVE (sev=0), peer CPU is NON-PARTICIPANT (sev=2)
MANHATTAN_OPTICAL platform with 131072 Kbytes of main memory

rommon 1 > switchover
System Bootstrap, Version 12.1(20010726:234219) [ffrazer-lh4 102], DEVELOPMENT S
OFTWARE
Copyright (c) 1994-1999 by cisco Systems, Inc.
Flash size is 16777216

Reset Reason Register = RESET_REASON_SW_NMI (0x4)

Reset type 0x2

Reading monitor variables from NVRAM
Running reset I/O devices
Enabling interrupts

Initializing TLB

Initializing cache

Initializing required TLB entries
Initializing main memory

SDRAM DIMM size 67108864

Sizing NVRAM

Initializing PCMCIA controller

Initializing SRC FPGA
CPU arbitration

→ This CPU is NON-PARTICIPANT (sev=2), peer CPU is ACTIVE (sev=0)
MANHATTAN_OPTICAL platform with 131072 Kbytes of main memory

rommon 1 >
```

Configuring Autoboot

If you have changed the default configuration register value from autoboot, you can change it back by performing the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **config-register 0x2102**	Sets the configuration register for autoboot.[1]
Step 2	Switch(config)# **boot system bootflash:***filename*	Sets the BOOT environment variable. This variable specifies the location and name of the system image file to use when automatically booting the system.
Step 3	Switch(config)# **end** Switch#	Returns to privileged EXEC mode.
Step 4	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration to NVRAM. The new configuration register value takes effect after the next system reload.

[1] This is the default configuration register setting. For details on using the configuration register to set boot parameters, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Note If the standby CPU switch module remains in ROM monitor mode, you can manually boot the CPU switch module using a system image either on the bootflash or on a Flash PC Card.

Example

The following example shows how to configure the Cisco ONS 15530 to autoboot using the first valid file on the Flash PC Card in slot 0:

```
Switch(config)# config-register 0x2102
Switch(config)# boot system flash slot0:
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
```

Displaying the Autoboot Configuration

To display the configuration register value, use the following EXEC command:

Command	Purpose
show version	Displays the configuration register value.
show bootvar	Displays the configuration register value.

Example

The following example shows the contents of the configuration register:

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) ONS-15530 Software (manopt-M0-M), Experimental Version 12.1(20010221:0]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 20-Feb-01 18:40 by lthanvan
Image text-base: 0x60010968, data-base: 0x604D8000

ROM: System Bootstrap, Version 12.1(20010204:232442) [vsankar-alarm_fix 106], DE
BOOTFLASH: M1540-ODS Software (manopt-M0-M), Experimental Version 12.1(20001229]

M1 uptime is 1 minute
System returned to ROM by power-on
System image file is "tftp://171.69.1.129//tftpboot/lthanvan/manopt-m0-mz"

cisco  (QUEENS-CPU) processor with 98304K/32768KB of memory.
R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

Last reset from unexpected value
2 Ethernet/IEEE 802.3 interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 64K).
➔ Configuration register is 0x2102
```

The following example shows the contents of the boot variable:

```
➔ Switch# show bootvar
BOOT variable = bootflash:ons15530-i-mz.1;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2

Standby auto-sync startup config mode is on

Standby auto-sync running config mode is on
```

Synchronizing the Configurations

During normal operation, the startup and running configurations are synchronized by default between the two CPU switch modules. In the event of a switchover, the new active CPU switch module uses the current running configuration. Configurations are synchronized either manually from the CLI using the **redundancy manual-sync** command or automatically following configuration changes input from the CLI or from SNMP if automatic synchronization is enabled.

Synchronizing Configurations Manually

To immediately synchronize the configurations used by the two CPU switch modules, use the following privileged EXEC command on the active CPU switch module:

Command	Purpose
redundancy manual-sync {**startup-config** | **running-config** | **both**}	Immediately synchronizes the configuration.

Example

The following example shows how to manually synchronize the running configuration:

```
Switch# redundancy manual-sync running-config
```

Enabling and Disabling Automatic Synchronization

You can enable and disable automatic synchronization of the running configuration and the startup configuration between the two CPU switch modules. Automatic synchronization ensures that, when a switchover occurs, the standby CPU switch module has the most recent configuration information.

Note By default, the Cisco ONS 15530 automatically synchronizes the running configuration and the startup configuration between the two CPU switch modules.

Table 3-3 lists the events that cause the automatic synchronization of the configuration files.

Table 3-3 Synchronization Events for Configuration Files

Filename	When Synchronized
running-config	Upon exiting from global configuration mode in the CLI, or within 5 seconds after an SNMP message that changes the configuration
startup-config	When a new configuration is copied to NVRAM on the active CPU switch module

To enable or disable the system to automatically synchronize the configurations on both CPU switch modules, perform the following steps on the active CPU switch module, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# [**no**] **auto-sync running-config**	Enables or disables synchronization of the running configuration when it is updated. The default state is enabled.
Step 3	Switch(config-red)# [**no**] **auto-sync startup-config**	Enables or disables synchronization of the startup configuration when it is updated. The default state is enabled.

Example

The following example shows how to disable automatic synchronization of the running configuration:

```
Switch(config)# redundancy
Switch(config-red)# no auto-sync running-config
Switch(config-red)# end
Switch# copy system:running-config nvram:startup-config
```

Configuring Maintenance Mode

You can configure the Cisco ONS 15530 to enter the redundancy maintenance mode. Configuration synchronizations and standby CPU switch module fault reporting are suppressed in maintenance mode. Upon exiting maintenance mode and reverting to redundant mode, the standby switch CPU switch module reboots to the hot-standby state.

Note When the system is in maintenance mode, switchovers only occur by entering the **redundancy switch-activity force** command, or physically removing the active CPU switch module.

To configure maintenance mode, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **maintenance-mode**	Configures the system in maintenance mode.

Example

The following example shows how to configure redundancy maintenance mode:

```
Switch(config)# redundancy
Switch(config-red)# maintenance-mode
This command will place the system in SIMPLEX mode [confirm] y
```

Displaying the CPU Switch Module Redundancy Configuration and Status

To display the CPU switch module redundancy configuration and status, use the following privileged EXEC commands:

Command	Purpose
show redundancy	Displays the redundancy configuration and status.
show redundancy capability	Displays capabilities of the active and standby CPU switch modules and the software version that is running.
show redundancy running-config-file	Displays the running configuration file on the standby CPU switch module. **Note** This command is only available on a terminal connected to the standby CPU switch module.

Examples

The following example shows the CPU switch module redundancy configuration and status:

```
Switch# show redundancy

Redundant system information
----------------------------
Available Uptime:             3 days, 4 hours, 35 minutes
Time since last switchover:   10 hours, 30 minutes
Switchover Count:             1

Inter-CPU Communication State:UP
Last Restart Reason:          Switch over
Software state at switchover: ACTIVE

Last Running Config sync:     2 hours, 18 minutes
Running Config sync status:   In Sync
Last Startup Config sync:     6 hours, 4 minutes
Startup Config sync status:   In Sync

This CPU is the Active CPU.
-------------------------------
Slot:                         7
Time since CPU Initialized:   22 hours, 33 minutes
Image Version:                ONS-15530 Software(ONS15530-I-M),...
Image File:                   bootflash:ons15530-i-mz.010727
Software Redundancy State:    ACTIVE
Hardware State:               ACTIVE
Hardware Severity:            0

Peer CPU is the Standby CPU.
-------------------------------
Slot:                         6
Time since CPU Initialized:   10 hours, 29 minutes
Image Version:                ONS-15530 Software(ONS15530-I-M),...
Image File (on sby-CPU):      bootflash:ons15530-i-mz.010727
Software Redundancy State:    STANDBY HOT
Hardware State:               STANDBY
Hardware Severity:            0
```

The following example shows the CPU switch module capabilities:

```
Switch# show redundancy capability
CPU capability support

 Active CPU  Sby CPU    Sby Compat        CPU capability description
 ---------- ---------- ----------- ----------------------------------------
    96 MB      96 MB   OK          CPU DRAM size
    32 MB      32 MB   OK          CPU PMEM size
   512 KB     512 KB   OK          CPU NVRAM size
    16 MB      16 MB   OK          CPU Bootflash size
    2.1        2.1     OK          CPU hardware major.minor version
    1.11       1.11    OK          CPU functional major.minor version

Linecard driver major.minor versions, (counts:Active=18, Standby=18)
```

```
 Active CPU  Sby CPU   Sby Compat  Drv ID     Driver description
 ---------- ---------- ----------- ------ ------------------------------------
    1.1        1.1     OK          0x1000 CPU w/o Switch Fabric
    1.1        1.1     OK          0x1001 Fixed Transponder, w/monitor
    1.1        1.1     OK          0x1002 Fixed Transponder, no monitor
    1.1        1.1     OK          0x1003 Pluggable Transponder, w/monitor
    1.1        1.1     OK          0x1004 Pluggable Transponder, no monitor
    1.1        1.1     OK          0x1005 Line Card Motherboard
    1.1        1.1     OK          0x1006 Backplane
 Active CPU  Sby CPU   Sby Compat  Drv ID     Driver description
 ---------- ---------- ----------- ------ ------------------------------------
    1.1        1.1     OK          0x1007 32-ch Mux/Demux
    1.1        1.1     OK          0x1008 Fixed 4-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x1009 Fixed 8-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100A Modular 4-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100B Modular 8-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100C 32-ch Array Wave Guide
    1.1        1.1     OK          0x100D Mux/Demux Motherboard
    1.1        1.1     OK          0x100E Modular 4-ch Mux/Demux plus OSC
    1.1        1.1     OK          0x100F Modular 8-ch Mux/Demux plus OSC
    1.1        1.1     OK          0x1010 Mux-Demux Motherboard, no OSC
    1.1        1.1     OK          0x1011 Line Card Motherboard, no splitter

Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts:Active=2, Standby=2

 Active CPU  Sby CPU   Sby Compat  Cl ID  Redundancy Client description
 ---------- ---------- ----------- ----- -------------------------------------
 ver  1-1   ver  1-1   OK          17    CPU Redundancy
 ver  1-1   ver  1-1   OK          6     OIR Client
```

The following example shows how to display the running configuration file on the standby CPU switch module:

```
sby-Switch# show redundancy running-config-file
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname Switch

<Information deleted>
```

Reloading the CPU Switch Modules

To reload one or both of the CPU switch modules, use the following privileged EXEC commands on the active CPU switch module CLI:

Command	Purpose
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both CPU switch modules in the shelf.

Example

The following example shows how to reload the standby CPU switch module:

```
Switch# redundancy reload peer
Reload peer [confirm] y
Preparing to reload peer
```

Configuring Privileged EXEC Mode Access on the Standby CPU Switch Module

Access to privileged EXEC mode from the standby CPU switch module CLI can be enabled from the active CPU switch module CLI. This feature provides extra security for the Cisco ONS 15530 system.

To configure access to privileged EXEC mode on the standby CPU switch module, perform the following steps on the active CPU switch module CLI, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **standby privilege-mode enable**	Enables access to privileged EXEC mode from the standby CPU switch module CLI. The default state is disabled.

Example

The following example shows how to configure redundancy maintenance mode:

```
Switch(config)# redundancy
Switch(config-red)# standby privilege-mode enable
```

Displaying the Standby CPU Switch Module Privileged EXEC Mode Status

To display the privileged EXEC mode access status on the standby CPU switch module, use the following privileged EXEC command:

Command	Purpose
show redundancy	Displays the redundancy configuration and status.

Example

The following example shows the privileged EXEC mode access status on the standby CPU switch module:

```
Switch# show redundancy


Redundant system information
----------------------------
Available Uptime:              15 hours, 27 minutes
sysUpTime (switchover clears): 15 hours, 27 minutes
Switchover Count:              0

Inter-CPU Communication State: DOWN
Last Restart Reason:           Normal boot

Last Running Config sync:      never
Running Config sync status:    Disabled
Last Startup Config sync:      never
Startup Config sync status:    Disabled

This CPU is the Active CPU.
-------------------------------
Slot:                          5
Time since CPU Initialized:    15 hours, 27 minutes
Image Version:                 ONS-15530 Software (ONS15530-I-M), Release 12.1(10)EV2
Image File:                    ons15530-i-mz.evt
Software Redundancy State:     ACTIVE
Hardware State:                ACTIVE
Hardware Severity:             0

Peer CPU is the Standby CPU.
-------------------------------
Slot:                          6
Time since CPU Initialized:    Unknown, peer CPU not responding
Image Version:                 Unknown, peer CPU not responding
Image File (on sby-CPU):       Unknown, peer CPU not responding
Software Redundancy State:     DISABLED
Hardware State:                NOT PLUGGED IN
Hardware Severity:             0
➔ Privilege Mode:              Enabled
```

About the Software Configuration Register

The Cisco ONS 15530 uses a 16-bit software configuration register to set specific system parameters. Settings for the software configuration register are written into NVRAM (nonvolatile random access memory).

You can change the software configuration register settings for the following reasons:

- Force the system into the ROM monitor or boot ROM
- Select a boot source and default boot filename
- Enable or disable the break function
- Control broadcast addresses
- Set the console terminal baud rate
- Load operating software from Flash memory

- Enable booting from a TFTP server
- Recover a lost password
- Boot the system manually using the **boot** command at the bootstrap program prompt.
- Force the system to boot automatically from the system bootstrap software (boot image) or from its default system image in onboard Flash memory, using any **boot system** commands stored in the startup configuration file in NVRAM

Software Configuration Register Settings

Table 3-4 describes each of the software configuration register bits.

⚠ **Caution** To avoid confusion and possibly halting the system, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table 3-4. For example, the value of 0x0101 is a combination of settings (bit 8 is 0x0100 and bits 00 through 03 are 0x0001).

Table 3-4 Software Configuration Register Bits

Bit Number	Hexadecimal	Description
00 to 03	0x0000 to 0x000F	Controls the system boot behavior (also known as the boot field)
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	Enables the OEM bit
08	0x0100	Disables the break function
09	0x0200	Uses secondary bootstrap during system boot
10	0x0400	Uses an IP broadcast with all zeros
11 to 12	0x0800 to 0x1000	Sets the console line speed (default is 9600 baud)
13	0x2000	Boots the default Flash software if network boot fails
14	0x4000	Uses IP broadcasts without network numbers
15	0x8000	Enables diagnostic messages and ignores the NVRAM contents

Bit 8 controls the console break function. Setting bit 8 (the factory default) causes the system to ignore the console break key. Clearing bit 8 causes the system to use the break key or break signal as a command to force the system into the bootstrap monitor (ROMMON), thereby halting normal operation. Regardless of the setting of the break enable bit, a break causes a return to the ROMMON during the first few seconds (approximately five seconds) of booting.

Bit 9 controls the secondary bootstrap program function. Setting bit 9 causes the system to use the secondary bootstrap. Clearing bit 9 (the factory default) causes the system to ignore the secondary bootstrap. The secondary bootstrap program is used for system debugging and diagnostics.

Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the system to use all zeros. Clearing bit 10 (the factory default) causes the system to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address.

Table 3-5 shows the combined effect of bits 14 and 10.

Table 3-5 Register Settings for Broadcast Address

Bit 14	Bit 10	Address (<net><host>)
0	0	<ones><ones>
0	1	<ones><zeros>
1	0	<net><ones>
1	1	<net><zeros>

Bit 12 and bit 11 in the configuration register determine the data transmission rate of the console terminal. Table 3-6 shows the bit settings for the four available rates. The factory-set default data transmission rate is 9600.

Table 3-6 Settings for Console Terminal Transmission Rate

Bit 12	Bit 11	Baud Rate
0	0	9600
0	1	4800
1	0	1200
1	1	2400

Bit 13 determines the system response to a bootload failure. Setting bit 13 (the factory default) causes the system to load operating software from bootflash memory after five unsuccessful attempts to load a boot file from the Flash memory device in slot 0. Clearing bit 13 causes the server to continue attempting to load a boot file from bootflash indefinitely.

Boot Field Values

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The order in which the system looks for system bootstrap information depends on the boot field setting in the configuration register.

Table 3-7 describes the values for the boot field.

Table 3-7 Configuration Register Boot Field Values

Boot Field Value	Description
0x0 (0-0-0-0)	Stays at the system bootstrap prompt. You must boot the operating system manually by giving a **boot** command to the ROMMON system bootstrap environment.
0x1 (0-0-0-1)	Boots the first system image in onboard Flash SIMM. If the boot fails, the system stops booting and remains in ROMMON mode.
0x2 (0-0-1-0) to 0xF (1-1-1-1)	Loads the system image specified by **boot system** commands in the startup configuration file. When the startup configuration file does not contain **boot system** commands, the system tries to load the first system image stored on the Flash memory device in slot 0. If that attempt fails, the system tries to boot with the first system image in bootflash. If that also fails, the system stops booting and remains in ROMMON mode. The factory default is 0x2.

Default System Boot Behavior

The factory default value for the configuration register on the Cisco ONS 15530 is 0x2102. When the system boots, the following occurs:

- The system attempts to load the system images specified in the **boot system** commands in the startup configuration file. If no **boot system** commands are configured, the system attempts to load the first system image stored on the Flash memory device in slot 0.
- The console Break key sequence, or break signal, is disabled and the system ignores it while rebooting.

Note Regardless of the setting of the break enable bit, a break causes a return to the ROMMON during the first few seconds (approximately five seconds) of booting.

- After five failed attempts to load a system image on the Flash memory device in slot 0, the system loads the first system image from Flash memory. If that attempt fails, the system stays in ROMMON mode.

Boot Command

You can enter only the **boot** command, or you can include additional boot instructions, such as the name of a file stored in Flash memory or a file that you specify for booting from a network server.

If you use the **boot** command without specifying a file or any other boot instructions, the system boots using the default system image (the first system image in onboard Flash memory). Otherwise, you can instruct the system to boot from a specific system image in Flash memory (using the **boot** *filename* command) or by sending a direct TFTP request to a specific server (using the **boot** *filename ip-address* command).

For more information on system booting, see Chapter 10, "Managing Your Cisco ONS 15530 System."

Changing the Software Configuration Register

To change the configuration register, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# **config-register** *value*	Sets the contents of the configuration register. The *value* is a hexadecimal number preceded by **0x**. See Table 3-4 for the list of values. **Note** The new configuration register value takes effect at the next system reload.
Step 3	Switch(config)# **end** Switch#	Returns to privileged EXEC mode.
Step 4	Switch# **reload**	(Optional) Reloads the system using the new configuration register value.

Note The factory default value for the register is 0x2102.

Example

The following example shows how to configure the system to manually boot from the ROMMON prompt:

```
Switch# configuration terminal
Switch(config)# config-register 0x100
Switch(config)# end
Switch# reload
```

Verify the Configuration Register Value

To verify the configuration register value, use the following EXEC command:

Command	Purpose
Switch# **show version**	Displays the current configuration register value. This value is used at the next system reload.

Example

The following example shows how to configure the system to examine the startup configuration file for boot system options:

```
Switch# show version

<Information deleted>

Configuration register is 0x2102 (will be 0x100 at next reload)
```

CHAPTER 4

Configuring ESCON Signal Aggregation

This chapter describes how to configure ESCON signal aggregation on 10-port ESCON multiplexing line cards and 10-Gbps ITU trunk cards on the Cisco ONS 15530. This chapter includes the following sections:

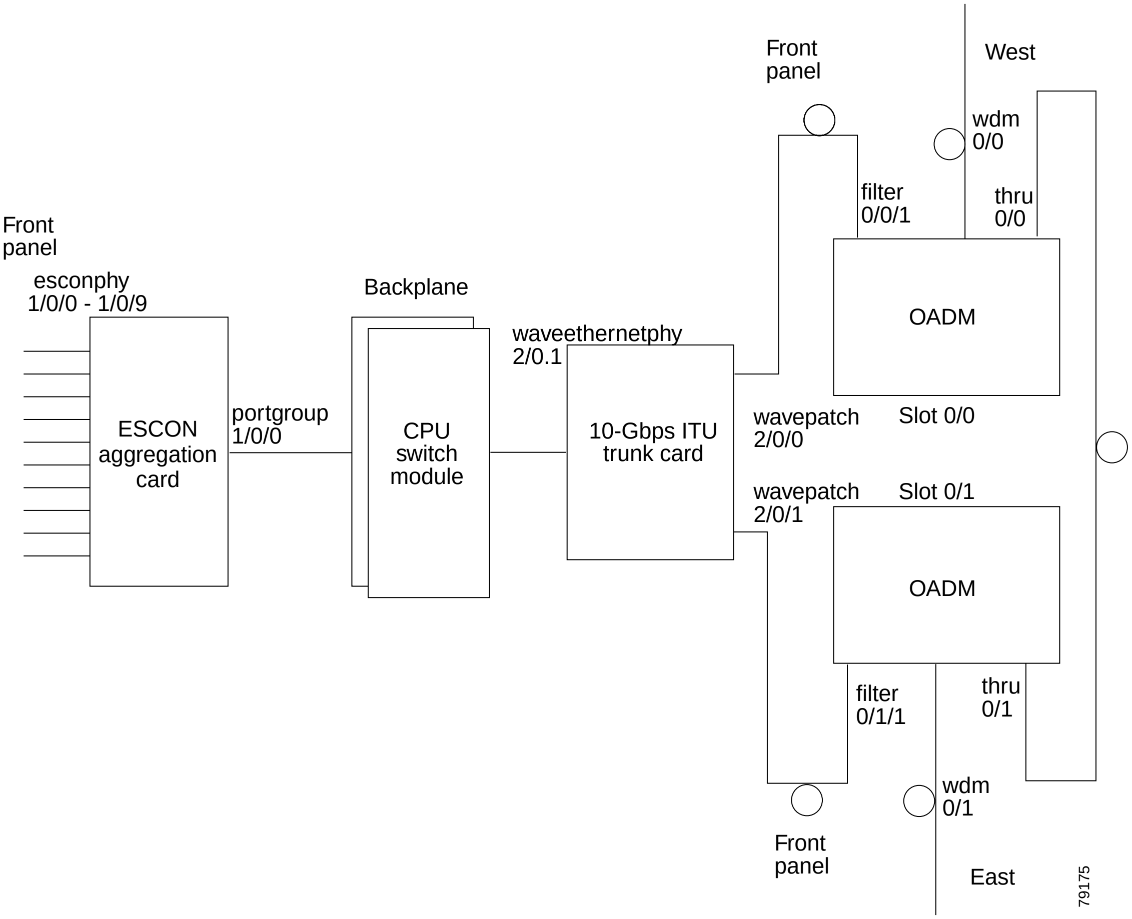
- About ESCON Signal Aggregation Support
- Configuring ESCON Multiplexing Line Card Interfaces
- Configuring 10-Gbps ITU Trunk Card Interfaces
- Configuring 10-GE Uplink Card Interfaces
- About Cross Connections
- About Alarm Thresholds
- Configuring Alarm Thresholds
- About Patch Connections
- Configuring Patch Connections

About ESCON Signal Aggregation Support

The ESCON multiplexing line card aggregates up to 10 ESCON data streams into a single 2.5-Gbps signal, which is transmitted through the switch fabric to a 10-Gbps ITU trunk card or a 10-GE uplink card. The 10-Gbps ITU trunk card converts up to four aggregated signals to one ITU wavelength and sends it to an OADM module. The 10-GE uplink card converts up to four aggregated signals into a 10-GE 1310-nm signal and sends it to a 10-GE client card on either a Cisco ONS 15540 ESP or Cisco ONS 15540 ESPx.

Figure 4-1 shows the path of an ESCON signal through the Cisco ONS 15530.

Figure 4-1 Interface Model for ESCON Aggregation



To configure ESCON support on the Cisco ONS 15530, perform the following steps:

Step 1 Configure ESCON multiplexing line card interfaces.

Step 2 Configure 10-Gbps ITU trunk card interfaces or 10-GE uplink card interfaces.

Step 3 Configure cross connections.

Step 4 Configure alarm thresholds (optional).

Step 5 Configure patch connections.

Configuring ESCON Multiplexing Line Card Interfaces

The ESCON multiplexing line card has two types of interfaces: 10 esconphy interfaces on the client side and one portgroup interface on the trunk side. The primary feature to configure on the ESCON multiplexing line card is the in-band message channel flow identifier. The in-band message channel provides an encapsulation that uniquely identifies an ESCON signal when it is aggregated with the other ESCON signals.

To configure the ESCON multiplexing line cards interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface esconphy** *slot*/**0**/*port* Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **cdl flow identifier** *number*	Configures the in-band message channel flow identifier. The range is 0 to 254. **Note** You must configure the other esconphy interface in the network that supports this signal with the same flow identifier. **Caution** Use unique flow identifiers for each esconphy interface on the system. Duplicate flow identifiers might interfere with APS switchovers.
Step 3	Switch(config-if)# **laser control forward enable**	Enables forward laser control on the interface. The default for esconphy interfaces is enabled.
Step 4	Switch(config-if)# **no shutdown**	Enables the interface.
Step 5	Switch(config-if)# **exit** Switch(config)#	Returns to global configuration mode. Repeat Step 1 through Step 5 for the other esconphy interfaces on the ESCON multiplexing line card.

Note When forward laser control is enable on an esconphy interface and a loss of light is detected on the port, the transmitter laser on the corresponding port on the remote node is turned off, regardless of the forward laser control configuration on the remote esconphy interface.

Example

The following example shows how to configure ESCON multiplexing line card interfaces:

```
Switch(config)# interface esconphy 10/0/0
Switch(config-if)# cdl flow identifier 100
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Displaying the ESCON Multiplexing Line Card Interface Configuration

To display the configuration of ESCON multiplexing line card interfaces, use the following EXEC command:

Command	Purpose
show interfaces {**esconphy** | **portgroup**} *slot*/*subcard*/*port*	Displays the interface configuration.

Example

The following example shows how to display the configuration of an esconphy interface:

```
Switch# show interfaces esconphy 7/0/0
EsconPhy7/0/0 is down, line protocol is down
  Signal quality:Loss of light
  Client Laser Status:Down due to Request from Remote
  Forward laser control:On
  Flow-identifier:40
  Configured threshold Group:escon
  Threshold monitored for:8b10b cvrd
  SF set value:10e-3 (20000 in 1 secs)
Threshold monitored for:CRC
  SF set value:10e-3 (19999 in 1 secs)
  Received Frames:0
  Transmit Frames:0
  Code violation and running disparity error count(cvrd):0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  CRC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  Egress Packet Sequence error count:0
  Egress Packet Indicated error count:0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
  Hardware is escon_phy_port
```

The following example shows how to display the configuration of a portgroup interface:

```
Switch# show interfaces portgroup 10/0/0
devt_ham_03/11#sh in portgroup 10/0/0
Portgroup10/0/0 is up, line protocol is up
  Transmit Packets: 883067943
  Received Packets: 887268737
  Code violation and running disparity error count(cvrd): 247499080
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  CRC error count: 3
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  CDL HEC error count: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  SII Mismatch error count: 0
  ESCON Protocol Mismatch error count: 0
  Hardware is portgroup
```

Configuring 10-Gbps ITU Trunk Card Interfaces

To configure the 10-Gbps ITU trunk card interface, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface waveethernetphy** *slot*/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [**no**] **loopback**	Enables or disables internal loopback for testing and defect isolation. (Optional)
Step 3	Switch(config-if)# [**no**] **laser shutdown**	Turns the laser on and off. (Optional) **Note** The laser must warm up for 2 minutes before carrying traffic.
Step 4	Switch(config-if)# [**no**] **cdl defect-indication force hop-endpoint**	Enables or disables hop endpoint for in-band message channel defect indications (Optional).
Step 5	Switch(config-if)# **no shutdown**	Enables the interface.
Step 6	Switch(config-if)# **exit** Switch(config)	Returns to global configuration mode.
Step 7	Switch(config)# **interface waveethernetphy** *slot*/**0.***subinterface* Switch(config-subif)#	Selects the subinterface to configure and enters interface configuration mode.
Step 8	Switch(config-subif)# **no shutdown**	Enables the interface.
Step 9	Switch(config-subif)# **exit** Switch(config)	Returns to global configuration mode.
Step 10	Switch(config)# **interface wavepatch** *slot*/**0**/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 11	Switch(config-if)# **optical threshold power receive** {**low** | **high**} {**alarm** | **warning**} *value* [**severity** {**critical** | **major** | **minor** | **not alarmed** | **not reported**}]	Specifies the optical power receive threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: –22 dBm Low warning: –20 dBm High warning: –8 dBm High alarm: –6 dBm Alarm severity: **major** Warning severity: **not alarmed**
Step 12	Switch(config-if)# [**no**] **shutdown**	Enables or disables the interface. Repeat Step 10 and Step 12 on **wavepatch** *slot*/**0**/**1** for splitter 10-Gbps ITU trunk cards.

Caution Loopbacks on waveethernetphy interfaces disrupt service. Use this feature with care.

Note For configuration information for the ethernetdcc interface, see the "Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel" section on page 9-12.

Example

The following example shows how to configure 10-Gbps ITU trunk card waveethernetphy interfaces:

```
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# cdl defect-indication force hop-endpoint
```

Displaying the 10-Gbps ITU Trunk Card Interface Configuration

To display the configuration of 10-Gbps ITU trunk card interfaces, use the following EXEC command:

Command	Purpose
show interfaces {**waveethernetphy** *slot*/**0**[.*subinterface*] | **wavepatch** *slot*/**0**/*port*}	Displays the interface configuration.

Examples

The following example shows how to display the configuration of a waveethernetphy interface:

```
Switch# show interfaces waveethernetphy 10/0
WaveEthernetPhy10/0 is down, line protocol is down
  Channel:30   Frequency:195.7 Thz   Wavelength:1531.90 nm
  Active Wavepatch       :Wavepatch10/0/1
  Splitter Protected     :No
  Signal quality         :Loss of lock
  Receive power level    :-35.0 dBm
  Laser Bias Current     :91 mA
  Laser Temperature      :31.0 degree C
  Laser shut down        :No
  Osc physical port      :No
  Wavelength used for inband management:No
  Loopback not set

  Configured threshold Group:None
  CDL HEC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  CRC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  Code violation and running disparity error count( 64b66b cvrd):0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0

  Defect Indication Status      :up
  Configured Node Behavior      :None
  Current Node Behavior         :Path Terminating
  Defect Indication Receive     :         None
  Defect Indication Transmit    :BDI-H
  Total Tx Frames Sent to N/W:  0
  Tx Gen CDL Idle Frame:        1843017892

  Rx Frames rcvd from N/W:      0
  Rx CRC Errors:                0
  Rx HEC Errors:                0
  Rx XGMII Errors:              0
  Rx IPG drpd pkts:             0
  Rx Idle Packets :             0
  Rx Oversize Frames :          0
  Rx Undersize Frames :         0

  Rx SII mismatch drpd data Frames :    0
  Rx SII mismatch drpd idle Frames :    0

  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

The following example shows how to display the configuration of a waveethernetphy subinterface:

```
Switch# show interfaces waveethernetphy 10/0.1
WaveEthernetPhy10/0.1 is down, line protocol is down

  Tx Frames Sent to N/W:        0
  Tx HEC Errors:                0
  Tx CRC Errors:                0
  Tx QuadPHY sybl Errs:         55688870321
  Tx Dropped Frames:            0
  Tx Oversize Frames:           0
  Tx Undersize Frames:          0
  Tx Rcvd Idle Packets:         0

  Rx Frames Sent to Clnt:       0
  Rx FIFO full drpd pkts:       0
  Rx Gen Idle pkt cnt:          0

  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

The following example shows how to display the configuration of a wavepatch interface:

```
Switch# show interfaces wavepatch 3/0/0
Wavepatch3/0/0 is up, line protocol is up
  Receiver power level:-9.86 dBm
  Optical threshold monitored for :Receive Power (in dBm)
  Threshold exceeded for :High Warning
  Low alarm value = -22.0  (default)
  Low Alarm Severity = major
  Low warning value = -20.0  (default)
  Low Warning Severity = not alarmed
  High alarm value = -8.0  (default)
  High Alarm Severity = major
  High warning value = -10.0  (default)
  High Warning Severity = not alarmed
  Hardware is passive_port
```

Configuring 10-GE Uplink Card Interfaces

To configure the 10-GE uplink card interface, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface tengigethernetphy** *slot*/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [**no**] **loopback**	Enables or disables internal loopback for testing and defect isolation. (Optional)
Step 3	Switch(config-if)# [**no**] **laser shutdown**	Turns the laser on and off. (Optional)
Step 4	Switch(config-if)# [**no**] **cdl defect-indication force hop-endpoint**	Enables or disables hop endpoint for in-band message channel defect indications (Optional).
Step 5	Switch(config-if)# [**no**] **shutdown**	Enables or disables the interface.
Step 6	Switch(config-if)# **exit** Switch(config)	Returns to global configuration mode.
Step 7	Switch(config)# **interface tengigethernetphy** *slot*/**0.***subinterface* Switch(config-subif)#	Selects the subinterface to configure and enters interface configuration mode.
Step 8	Switch(config-subif)# [**no**] **shutdown**	Enables or disables the interface.
Step 9	Switch(config-subif)# **exit** Switch(config)	Returns to global configuration mode.
Step 10	Switch(config)# **interface wavepatch** *slot/subcard/port* Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 11	Switch(config-if)# **no shutdown**	Enables the interface.

Caution Loopbacks on tengigethernetphy interfaces disrupt service. Use this feature with care.

Note For configuration information for the ethernetdcc interface, see the "Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel" section on page 9-12.

Example

The following example shows how to configure 10-GE uplink card interfaces:

```
Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# cdl defect-indication force hop-endpoint
```

Displaying the 10-GE Uplink Card Interface Configuration

To display the configuration of 10-GE uplink card interfaces, use the following EXEC command:

Command	Purpose
show interfaces {tengigethernetphy *slot*/**0**[**.***subinterface*] | **wavepatch** *slot*/**0**/*port*}	Displays the interface configuration.

Example

The following example shows how to display the configuration of an tengigethernetphy interface:

```
Switch# show interfaces tengigethernetphy 3/0
TenGigEthernetPhy3/0 is up, line protocol is up
  Signal quality       :Good
  laser shut down      :Off
  Osc physical port    :No
  Loopback not set
  Wavelength used for inband management:No

  Configured threshold Group:None
  CDL HEC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  CRC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  Code violation and running disparity error count( 64b66b cvrd):0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0

  Defect Indication Status      :up
  Configured Node Behavior      :None
  Current Node Behavior         :Path Terminating
  Defect Indication Receive     :         None
  Defect Indication Transmit    :         None

  Total Tx Frames Sent to N/W:  48297
  Tx Gen CDL Idle Frame:        2173636535

  Rx Frames rcvd from N/W:      0
  Rx CRC Errors:                0
  Rx HEC Errors:                0
  Rx XGMII Errors:              0
  Rx IPG drpd pkts:             0
  Rx Idle Packets :             1836560218
  Rx Oversize Frames :          0
  Rx Undersize Frames :         0

  Rx SII mismatch drpd data Frames :    0
  Rx SII mismatch drpd idle Frames :    1842816773

  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

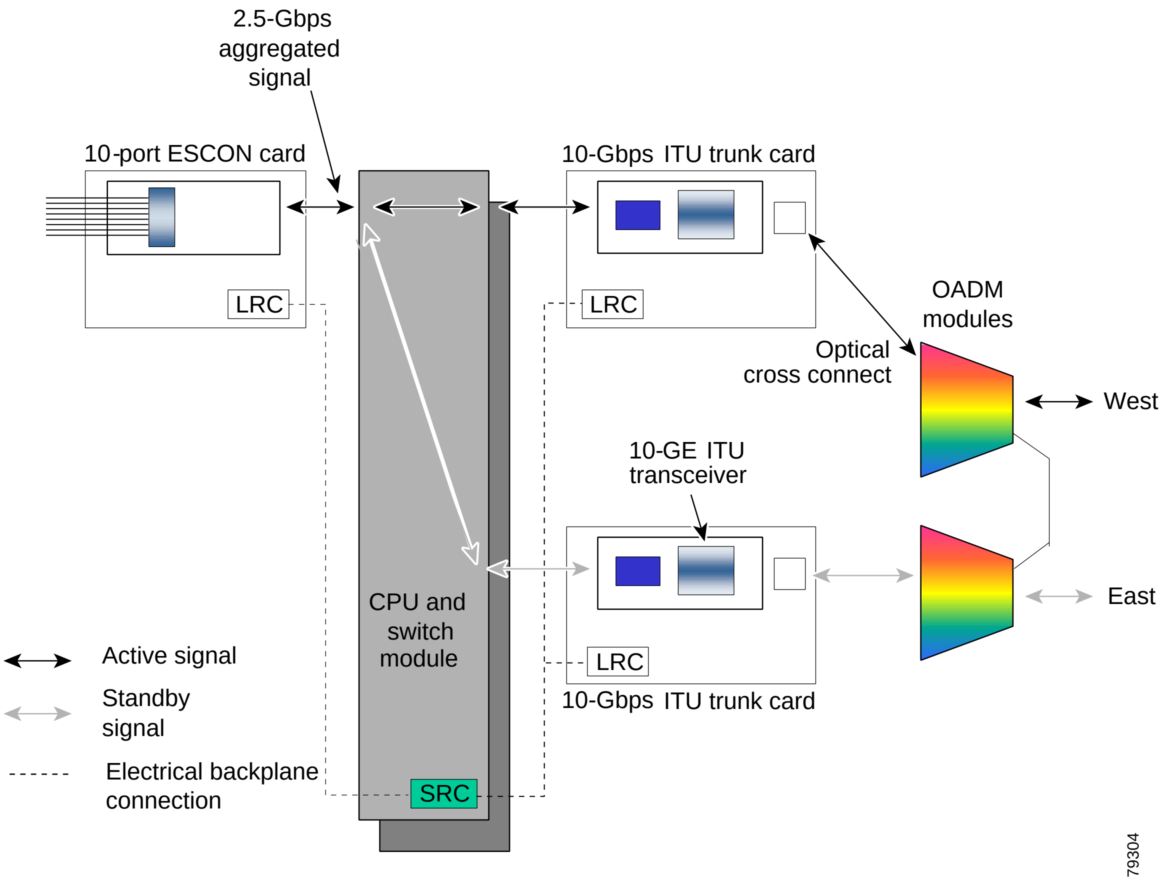
The following example shows how to display the configuration of a tengigethernetphy subinterface:

```
Switch# show interfaces tengigethernetphy 3/0.4
TenGigEthernetPhy3/0.4 is up, line protocol is up

  Tx Frames Sent to N/W:        0
  Tx HEC Errors:                0
  Tx CRC Errors:                0
  Tx QuadPHY sybl Errs:         37831687439
  Tx Dropped Frames:            0
  Tx Oversize Frames:           0
  Tx Undersize Frames:          0
  Tx Rcvd Idle Packets:         0

  Rx Frames Sent to Clnt:       0
  Rx FIFO full drpd pkts:       0
  Rx Gen Idle pkt cnt:          0

  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15530. Figure 4-2 shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 4-2 Optical Cross Connection Example



Configuring Cross Connections

The aggregated signal from the ESCON multiplexing line cards passes through the switch fabric to the 10-Gbps ITU trunk card or the 10-GE uplink card. To establish a cross connection through the switch fabric, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **connect** *interface1 interface2*	Creates a cross connection between two interfaces through the switch fabric.

Example

The following example shows how to configure a cross connection between an ESCON multiplexing line card and a 10-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0.1
```

The following example shows how to configure a cross connection between an ESCON multiplexing line card and a 10-GE uplink card:

```
Switch(config)# connect portgroup 2/0/0 tengigethernetphy 3/0.1
```

Displaying the Cross Connection Configuration

To display the cross connection configuration, use the following privileged EXEC command:

Command	Purpose
show connect [**edge** | **intermediate** [**sort-channel** | **interface** *interface*]]	Displays the signal cross connection configuration through the system.

Examples

The following example shows the cross connections within a system for an ESCON signal:

```
Switch# show connect
Index Client Intf     Trunk Intf      Kind        C2TStatus  T2CliStatus
----- --------------- --------------- ----------- ----------  ---------
15    Port3/0/0       WaveE8/0.1      Provisioned Up         Up
```

The following example shows the cross connections within a system for a transponder signal:

```
Switch# show connect intermediate
client/       wave          wave               wdm
wave          client        patch   filter   trk  channel
------------  ------------  -------  ------  ----- -------
Trans7/0/0    Wave7/0       7/0/0*  0/0/0    0/0    25
                            7/0/1
```

About Alarm Thresholds

You can configure thresholds on ESCON multiplexing line card, 10-Gbps ITU trunk card, and 10-GE uplink interfaces that issue alarm messages to the system if the thresholds are exceeded.

Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

Configuring Alarm Thresholds

To configure alarm thresholds on ESCON multiplexing line card, 10-Gbps ITU trunk card, and 10-GE uplink interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **threshold-list** *name* Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode.
Step 2	Switch(config-t-list)# **notification-throttle timer** *seconds*	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)
Step 3	Switch(config-t-list)# **threshold name** {**8b10b cvrd** | **cdl hec** | **crc**} {**failure** | **degrade**} [**index** *value*] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# **value rate** *value*	Specifies the threshold rate value. This value is the negative power of 10 (10^{-n}).
Step 5	Switch(config-threshold)# **description** *text*	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# **exit** Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 6 to configure more thresholds in the threshold list.
Step 7	Switch(config-t-list)# **exit** Switch(config)#	Returns to global configuration mode.
Step 8	Switch(config)# **interface** *interface* Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 9	Switch(config-if)# **threshold-group** *name*	Configures the threshold list on the interface.

Note Only one threshold list can be associated with the interfaces on an ESCON multiplexing line card.

Table 4-1 lists the threshold error rates in errors per second for ESCON signals.

Table 4-1 Threshold Values for Monitored Rates for ESCON Signals (Errors Per Second)

Rate	ESCON CRC	ESCON CVRD	10 Gigabit Ethernet CVRD	10 Gigabit Ethernet CDL HEC
3	19999	20000	12,443,900	6512
4	19999	20000	1,249,438	665
5	1999	2000	124,944	67
6	199	200	10,312	7
7	20	20	1031	0.7

Table 4-1 Threshold Values for Monitored Rates for ESCON Signals (Errors Per Second) (continued)

Rate	ESCON CRC	ESCON CVRD	10 Gigabit Ethernet CVRD	10 Gigabit Ethernet CDL HEC
8	2	2	103	0.07
9	0.2	0.2	10	0.007

Example

The following example shows how to create an alarm threshold list and configure that list for ESCON multiplexing line card interfaces:

```
Switch# configure terminal
Switch(config)# threshold-list escon-counters
Switch(config-t-list)# threshold name crc degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name crc failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface esconphy 3/0/0
Switch(config-if)# threshold-group escon-counters
```

Displaying the Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for an esconphy interface, use the following EXEC commands:

Command	Purpose
show threshold-list [*name*]	Displays the threshold group configuration.
show interfaces {**esconphy** *slot*/*subcard*/*slot* | **waveethernetphy** *slot*/*subcard* | **tengigethernetphy** *slot*/*subcard*}	Displays the interface configuration.

Examples

The following example shows how to display the configuration of a threshold group:

```
Switch# show threshold-list escon-counters

 Threshold List Name: escon-counters
   Notification throttle timer : 5 (in secs)
   Threshold name : CRC  Severity : Degrade
      Value : 10e-9
      APS Trigger : Not set
   Threshold name : CRC  Severity : Failure
      Value : 10e-7
      APS Trigger : Not set
```

The following example shows how to display the threshold group information for an interface:

```
Switch# show interfaces esconphy 3/0/0
EsconPhy3/0/0 is up, line protocol is up
  Signal quality: Good
  Forward laser control: Off
  Configured threshold Group: escon-counters
  Threshold monitored for: CRC
  SF set value: 10e-7 (20 in 1 secs)
  SD set value: 10e-9 (1 in 5 secs)
  Received Frames: 0
  Transmit Frames: 0
  Code violation and running disparity error count(cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  CRC error count: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Egress Packet Sequence error count: 0
  Egress Packet Indicated error count: 0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
  Hardware is escon_phy_port
```

About Patch Connections

Because the mux/demux modules are passive devices, the Cisco ONS 15530 does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connection configuration using the CLI.

Configuring Patch Connections

To configure patch connections between link cards within the same shelf, use the following global configuration commands:

Command	Purpose
patch wavepatch *slot1*/*subcard1*/*port1* **filter** *slot2*/*subcard2*/*port2* or **patch filter** *slot1*/*subcard1*/*port1* **wavepatch** *slot2*/*subcard2*/*port2*	Configures the patch connection between a 10-Gbps ITU trunk card and an OADM module.
patch thru *slot*/*subcard1* **thru** *slot*/*subcard2*	Configures the patch connection between two OADM modules.
patch wave *slot*/*subcard* **oscfilter** *slot*/*subcard* or **patch oscfilter** *slot*/*subcard* **wave** *slot*/*subcard*	Configures the patch connection between the wave interface on the OSC module and the oscfilter interface on the OADM module. This is only required if an OSC module is present.

Note If you correctly patch your cards, **patch** command configuration is not necessary for the signal to pass from the client to the trunk fiber.

Example

The following example shows how to configure the patch connections between line cards in a shelf with two OSC cards in slot 4, two OADM modules with OSC in slot 0, and a splitter 10-Gbps ITU trunk card in slot 3:

```
Switch# configure terminal
Switch(config)# patch thru 0/0 thru 0/1
Switch(config)# patch wave 4/0 oscfilter 0/0
Switch(config)# patch wave 4/1 oscfilter 0/1
Switch(config)# patch wavepatch 3/0/0 filter 0/0/1
Switch(config)# patch wavepatch 3/0/1 filter 0/1/1
```

Displaying Patch Connections

To display the patch connections, use the following privileged EXEC command:

Command	Purpose
show patch [**detail**]	Displays the patch connections.

Note The error field in the **show patch** command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a transponder card and an OADM module, “Channel Mismatch” appears for the patch connection. When more than one OADM module drops the same channels, “Channel Mismatch” appears for all patch connections.

Example

The following example shows the patch connections:

```
Switch# show patch

Patch Interface    Patch Interface    Type    Error
---------------    ---------------    ----    -----
Thru0/0            Thru0/1            USER
Wave3/0            Oscfilter0/0       USER
Wave3/1            Oscfilter0/1       USER
```

Configuring Transponder Line Card Interfaces

This chapter describes how to configure interfaces and patch connections on the Cisco ONS 15530. This chapter includes the following sections:

To configure transparent interfaces on the Cisco ONS 15530, perform the following steps:

Step 1 Specify the protocol encapsulation and, if required, the transmission rate and OFC (open fiber control), or specify the signal clock rate (required).

Step 2 Specify the laser frequency (optional).

Step 3 Enable protocol monitoring (optional).

Step 4 Create alarm threshold lists and apply them to the interfaces (optional).

Step 5 Enable forward laser control (optional).

To configure wave interfaces on the Cisco ONS 15530, perform the following steps:

Step 1 Enable forward laser control (optional).

Step 2 Enable laser safety protocol (optional).

To configure patch connections on the Cisco ONS 15530, perform the following steps:

Step 1 Configure the patch connections between the OADM modules and the wavepatch interface of the transponder line card (required).

Step 2 Configure the patch connections between the OSC (optical supervisory channel) interface on the OADM modules and the wavepatch interface of the OSC (required if the OSC is present).

Configuring Protocol Encapsulation or Clock Rate

A transparent interface does not terminate the protocol of the signal it receives, but it does convert it from an optical signal to an electrical signal and back to an optical signal. Therefore, you must configure the signal transmission rate by specifying either the protocol encapsulation or the clock rate.

To configure the protocol encapsulation or the clock rate for a transparent interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface transparent** *slot*/*subcard*/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **encapsulation** {**fastethernet** | **fddi** | **gigabitethernet** | **escon**} or	Specifies Fast Ethernet, FDDI, Gigabit Ethernet, or ESCON. OFC[1] is disabled.
	Switch(config-if)# **encapsulation sysplex clo** or	Specifies Sysplex CLO[2]. OFC is disabled. Forward laser control is enabled on both the transparent and wave interfaces. OFC is disabled.
	Switch(config-if)# **encapsulation sysplex etr** or	Specifies Sysplex ETR[3]. OFC is disabled.
	Switch(config-if)# **encapsulation sysplex isc** {**compatibility** | **peer**} or	Specifies ISC[4] compatibility mode (1 Gbps) or peer mode (2 Gbps). OFC is enabled for compatibility mode and disabled for peer mode.
	Switch(config-if)# **encapsulation ficon 1g** or	Specifies FICON. OFC is disabled.
	Switch(config-if)# **encapsulation sonet** {**oc3** | **oc12** | **oc48**} or	Specifies SONET as the signal protocol and OC-3, OC-12, or OC-48 as the transmission rate. OFC is disabled.
	Switch(config-if)# **encapsulation sdh** {**stm-1** | **stm-4** | **stm-16**} or	Specifies SDH as the signal protocol and STM-1, STM-4, or STM-16 as the transmission rate. OFC is disabled.
	Switch(config-if)# **encapsulation fibrechannel** {**1g** | **2g**} [**ofc** {**enable** | **disable**}] or	Specifies Fibre Channel as the signal protocol and 1 Gbps or 2 Gbps as the transmission rate. Enables or disables OFC. OFC is disabled by default.
	Switch(config-if)# **clock rate** *value*	Specifies the signal transmission clock rate without an associated protocol. OFC is disabled. **Note** Protocol monitoring cannot be enabled on the interface when the **clock rate** command is configured.

[1] For information about OFC, see the "About Laser Shutdown" section on page 5-13.

[2] CLO = control link oscillator

[3] ETR = external timer reference

[4] ISC = Intersystem Channel Links

Note Disable autonegotiation 2-Gbps Fibre Channel client equipment connected to Cisco ONS 15530 and set the speed to match the clock rate or protocol encapsulation set on transparent interfaces. The transponder line cards only recognize the configured clock rate or protocol encapsulation and do not support autonegotiation.

Caution Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Sysplex CLO and Sysplex ETR are supported outside the nominal range of the clock rates for the Cisco ONS 15530 because of the nature of the traffic type.

Table 5-1 lists the clock rates for well-known protocols supported by the transponder line card:

Table 5-1 Supported Clock Rates for Well-Known Protocols

Well-Known Protocol	Clock Rate (in kbps)
DS3	44,736
DV1[1] in ADI[2] mode	270,000
E3	34,368
ESCON	200,000
Fibre Channel (1 Gbps)	1,062,500
Fibre Channel (2 Gbps)	2,125,000
FICON (1 Gbps)	1,062,500
FICON (2 Gbps)	2,125,000
Gigabit Ethernet	1,250,000
ISC Compatibility Mode (ISC-1)	1,062,500
ISC Peer Mode (ISC-3)	2,125,000
SONET OC-1	51,840
SONET OC-3/SDH STM-1	155,520
SONET OC-12/SDH STM-4	622,080
SONET OC-24/SDH STM-8	933,120
SONET OC-48SDH STM-16	2,488,320

[1] DV = digital video

[2] ADI = Asynchronous Digital Interface

Note Error-free transmission of some D1 video signals (defined by the SMPTE 259M standard) and test patterns (such as Matrix SDI) cannot be guaranteed by the Cisco ONS 15500 Series because of the pathological pattern in D1 video. This well-known limitation is usually overcome by the D1 video equipment vendor, who uses a proprietary, second level of scrambling. No standards exist at this time for the second level of scrambling.

Note Use the encapsulation command for clock rates supported by protocol monitoring rather than the clock rate command. For more information protocol monitoring, see the "About Protocol Monitoring" section on page 5-7.

Note When you must use Sysplex CLO encapsulation or Sysplex ETR encapsulation, you must configure APS bidirectional path switching. For more information on APS and bidirectional path switching, see Chapter 7, "About Splitter Protection."

Examples

The following example shows how to configure GE (Gigabit Ethernet) encapsulation on a transparent interface:

```
Switch(config)# interface transparent 10/0/0
Switch(config-if)# clock rate 1065
```

Note Removing the protocol encapsulation or the clock rate does not shut down the transmit lasers. To shut down the lasers, use the **shutdown** command.

Displaying Protocol Encapsulation or Clock Rate Configuration

To display the protocol encapsulation configuration of a transparent interface, use the following EXEC command:

Command	Purpose
show interfaces transparent *slot*/*subcard*/**0**	Displays the transparent interface configuration.

Examples

The following example shows how to display the protocol encapsulation configuration of a transparent interface:

```
Switch# show interfaces transparent 8/0/0
Transparent11/3/0 is administratively up, line protocol is up
  Encapsulation: GigabitEthernet
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change 00:00:03
  Forward laser control: Off
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 00:00:03
  Hardware is transparent
```

The following example shows how to display the clock rate configuration of a transparent interface:

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is administratively up, line protocol is up
  Encapsulation: Unknown
  Clock rate: 1000000 KHz
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change never
  Forward laser control: Off
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is transparent
```

About Transponder Line Card Channel Frequencies

The transponder line card supported by the Cisco ONS 15530 is tunable to one of two frequencies. These frequencies are adjacent on the ITU grid. For example, a transponder line card can support the frequencies for channel 5 and channel 6, but not for channel 5 and channel 8. By default, the transponder line card operates at the laser frequency for the lower channel number. However, you can configure the transponder line card to operate at the laser frequency for the higher channel number using the CLI.

Configuring Transponder Line Card Channel Frequency

To select the desired channel frequency for the transponder line cards supported by the Cisco ONS 15530, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface wave** *slot/subcard* Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **laser frequency** *number*	Selects one of the two frequencies in GHz supported by the laser. The default is the lower frequency for the transponder module.

Note The laser requires approximately 10 seconds to change to the new frequency and stabilize. Any **laser frequency** commands entered during this time are ignored.

Example

The following example shows how to change the transponder line card channel frequency:

```
Switch(config)# interface wave 10/0
Switch(config-if)# laser frequency 195700
```

Displaying Transponder Line Card Channel Frequency

To display the channel frequency configuration, use the following EXEC command:

Command	Purpose
show interfaces wave *slot*/*subcard*	Displays the wave interface configuration.

Example

The following example shows how to display the transponder line card channel frequency:

```
Switch# show interface wave 10/0
Wave10/0 is down, line protocol is down
  Channel: 30   Frequency: 195.7 Thz    Wavelength: 1531.90 nm
  Active Wavepatch : Wavepatch10/0/0
  Splitter Protected: No
  Signal quality: Loss of light
  Receiver power level:
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
```

About Protocol Monitoring

Transparent interfaces on the Cisco ONS 15530 can be configured to monitor protocol and signal performance. When monitoring is enabled, the system maintains statistics that are used to determine the quality of the signal.

The following protocols can be monitored:

- ESCON (Enterprise Systems Connection)
- Fibre Channel (1 Gbps only)
- FICON (Fiber Connection) (1 Gbps only)
- Gigabit Ethernet
- SDH (Synchronous Digital Hierarchy) (STM-1, STM-4, STM-16)
- SONET (OC-3, OC-12, OC-48)
- ISC (compatibility mode only)

Note Enabling monitoring on a transparent interface also enables monitoring on the corresponding wave interface. For example, if you enable monitoring on transparent interface 3/0/0, monitoring is also enabled on wave interface 3/0.

For Gigabit Ethernet, Fibre Channel, and FICON, the Cisco ONS 15530 monitors the code violation and running disparity error count.

For SONET errors, the Cisco ONS 15530 monitors the SONET section overhead only, not the SONET line overhead. Specifically, the Cisco ONS 15530 monitors the B1 byte and the framing bytes. The system can detect the following defect conditions:

- Loss of light
- Loss of lock (when the clock cannot be recovered from the received data stream)
- Severely errored frame
- Loss of frame

For SONET performance, the system monitors the B1 byte, which is used to compute the four SONET section layer performance monitor parameters:

The definitions for these acronyms come from the Telcordia SONET standard spec page 6-110.

- SEFS-S (second severely errored framing seconds)
- CV-S (section code violations)
- ES-S (section errored seconds)
- SES-S (section severely errored seconds)

Configuring Protocol Monitoring

To configure protocol monitoring on a transparent interface, and its corresponding wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface transparent** *slot*/*subcard*/**0** Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **monitor enable**	Enables signal monitoring. **Note** Protocol encapsulation must be configured on the transparent interface before enabling monitoring.

Examples

The following example shows how to enable protocol monitoring on a transparent interface:

```
Switch(config)# interface transparent 10/0/0
Switch(config-if)# monitor enable
```

The following example shows how to disable protocol monitoring on a transparent interface:

```
Switch(config)# interface transparent 10/0/0
Switch(config-if)# no monitor
```

Displaying Protocol Monitoring Configuration

To display the protocol monitoring configuration of a transparent interface, use the following EXEC command:

Command	Purpose
show interfaces {transparent *slot*/*subcard*/**0** | **wave** *slot*/*subcard*}	Displays the transparent interface configuration.

Examples

The following example shows how to display the protocol monitoring configuration of a transparent interface:

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is administratively up, line protocol is up
  Encapsulation: Sonet    Rate: oc3
➔ Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: None
➔ Section code violation error count(bip1): 3714369135
➔ Number of errored seconds(es): 57209
➔ Number of severely errored seconds(ses): 57209
➔ Number of severely errored framing seconds(sefs): 0
➔ Number of times SEF alarm raised: 0
➔ Number of times SF threshold exceeded: 0
➔ Number of times SD threshold exceeded: 384
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is transparent
```

The following example shows how to display the protocol monitoring configuration of a wave interface:

```
Switch# show interfaces wave 7/0
Wave7/0 is up, line protocol is up
  Channel: 31   Frequency: 195.8 Thz    Wavelength: 1531.12 nm
  Active Wavepatch : Wavepatch7/0/0
  Splitter Protected: No
  Signal quality: Good
  Receiver power level: -14.71 dBm
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 09:20:01
  Hardware is data_only_port
```

About Alarm Thresholds

You can configure thresholds on transparent and wave interfaces that issue alarm messages to the system if the thresholds are exceeded. The threshold values are applied to both transparent and wave interfaces on a transponder line card when protocol monitoring is enabled on the transparent interface.

The rate is based on the protocol encapsulation or the clock rate for the interface. Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

Configuring Alarm Thresholds

To configure alarm thresholds on transparent interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **threshold-list** *name* Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode.
Step 2	Switch(config-t-list)# **notification-throttle timer** *seconds*	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)
Step 3	Switch(config-t-list)# **threshold name** {**8b10b cvrd** | **cdl hec** | **sonet-sdh section cv**} {**failure** | **degrade**} [**index** *value*] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# **value rate** *value*	Specifies the threshold rate value. This value is the negative power of 10 (10^{-n}).
Step 5	Switch(config-threshold)# **description** *text*	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# **aps trigger**	Enables APS switchover when this threshold is crossed. (Optional) **Note** This command only triggers switchovers for y-cable protection, not for splitter protection.
Step 7	Switch(config-threshold)# **exit** Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 7 to configure more thresholds in the threshold list.
Step 8	Switch(config-t-list)# **exit** Switch(config)#	Returns to global configuration mode.
Step 9	Switch(config)# **interface** {**transparent** *slot*/*subcard*/**0** | **wave** *slot*/*subcard*} Switch(config-if)#	Selects the transparent or wave interface to configure and enters interface configuration mode.
Step 10	Switch(config-if)# **threshold-group** *name*	Configures the threshold list on the interface.

Note If a threshold type does not apply to the encapsulation type for the interface, that threshold type is ignored.

Table 5-2 lists the threshold error rates in errors per second for each of the protocol encapsulations.

Table 5-2 Thresholds for Monitored Protocols (Errors Per Second)

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON[1]	Fibre Channel[2]	ISC[3]
3	31,753	32,000	32,000	1,244,390	199,102	1,057,731	1,057,731	1,057,731
4	12,318	27,421	31,987	124,944	19,991	106,202	106,202	106,202
5	1518	5654	17,296	12,499	2000	10,625	10,625	10,625
6	155	616	2394	1250	200	1062	1062	1062
7	15.5	62	248	125	20	106	106	106
8	1.55	6.2	24.8	12.5	2	10.6	10.6	10.6
9	0.155	0.62	2.48	1.25	0.2	1.06	1.06	1.06

[1] One Gbps rate only.

[2] One Gbps rate only.

[3] Compatibility mode only.

[3] Rate is limited by the hardware.

Examples

The following example shows how to create an alarm threshold list and configure that list on a transparent interface:

```
Switch# configure terminal
Switch(config)# threshold-list sonet-counters
Switch(config-t-list)# threshold name sonet-sdh section cv degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface transparent 10/0/0
Switch(config-if)# threshold-group sonet-counters
```

The following example shows how to create an alarm threshold list with the APS switchover trigger and configure that list on a pair of associated transparent interfaces:

```
Switch(config)# threshold-list sonet-alarms
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 6
Switch(config-threshold)# aps trigger
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# redundancy
Switch(config-red)# associate group sonet-channel
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 5/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps revertive
Switch(config-red-aps)# enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 3/0/0
Switch(config-if)# encapsulation sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
Switch(config-if)# exit
Switch(config)# interface transparent 5/0/0
Switch(config-if)# encapsulation sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
```

Displaying Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for a transparent or wave interface, use the following EXEC commands:

Command	Purpose
show threshold-list [*name*]	Displays the threshold group configuration.
show interfaces {**transparent** *slot*/*subcard*/**0** | **wave** *slot*[/*subcard*]}	Displays the transparent or wave interface configuration.

Examples

The following example shows how to display the configuration of a threshold group:

```
Switch# show threshold-list sonet-counters

Threshold List Name: sonet-counters
   Notification throttle timer : 5 (in secs)
   Threshold name : sonet-sdh section cv         Severity : Degrade
      Value : 10e-9
      APS Trigger : Not set
      Description : SONET BIP1 counter
   Threshold name : sonet-sdh section cv         Severity : Failure
      Value : 10e-6
      APS Trigger : Set
      Description : SONET BIP1 counter
```

The following example shows how to display the threshold group information for an interface:

```
Switch# show interfaces transparent 3/0/0
Transparent3/0/0 is administratively up, line protocol is up
  Encapsulation: Sonet    Rate: oc3
  Signal monitoring: on
  Forward laser control: Off
➔ Configured threshold Group: sonet-counters
➔ Threshold monitored for: sonet-sdh section cv
➔ SF set value: 10e-8 (155 in 100 secs)
➔ SD set value: 10e-9 (155 in 1000 secs)
  Section code violation error count(bip1): 3713975925
  Number of errored seconds(es): 57203
  Number of severely errored seconds(ses): 57203
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 378
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is transparent
```

About Laser Shutdown

To avoid operator injury or transmission of unreliable data, or to provide quick path switchover, the Cisco ONS 15530 supports mechanisms to automatically shut down transponder line card lasers. The three types of laser shutdown mechanisms are:

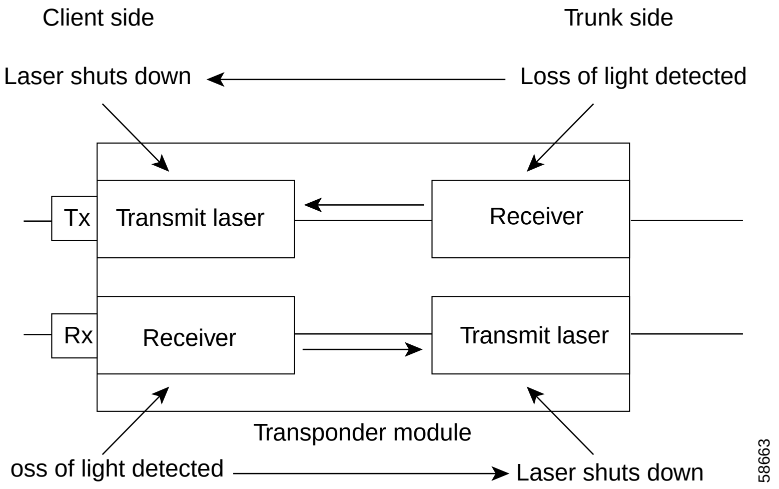
- Forward laser control
- OFC safety protocol
- Laser safety control

About Forward Laser Control

When loss of light occurs on the receive signal of a transparent or wave interface, the corresponding transmitting laser on the other side of the transponder line card continues to function and might send unreliable information to the client. Forward laser control provides a means to quickly shut down a transmitting laser when such a receive signal failure occurs (see Figure 5-1). The receive signal loss of light can result from a failure in the client equipment, a receiver failure in the transponder line card, or a laser shutdown on another node in the network.

This feature is convenient for configurations, such as Sysplex, where signal protection is performed in the client hardware and a quick laser shutdown causes a quick path switchover.

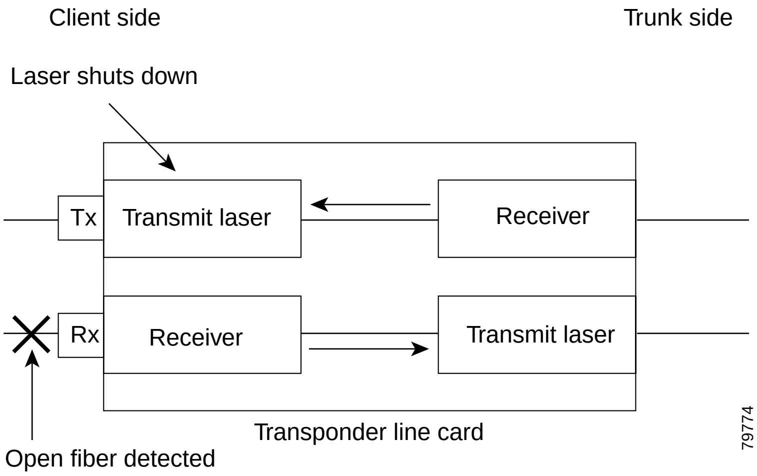
Figure 5-1 Forward Laser Control Overview



About OFC

The Cisco ONS 15530 allows you to enable the OFC safety protocol on the client side interfaces. When the system detects an "open fiber," the laser that transmits to the client equipment shuts down. An open fiber condition occurs when the connectors to the client equipment are detached from the transponder line card ports or when the fiber is cut (see Figure 5-2).

Figure 5-2 OFC Overview



The OFC safety protocol conforms to the Fibre Channel standard. It applies only to the Fibre Channel and ISC compatibility mode encapsulations. The Cisco ONS 15530 interoperates with OFC-standard-compliant client equipment.

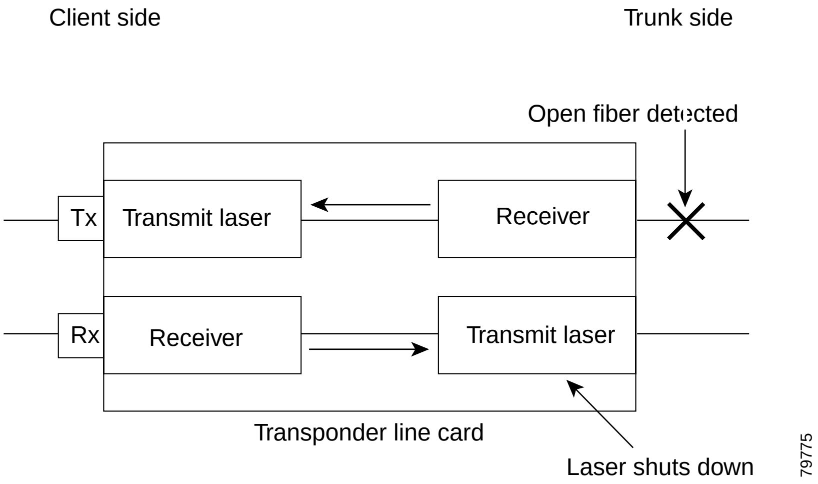
Caution Do not configure OFC with either forward laser control or laser safety control. Combining these features interferes with the OFC protocol.

Use the **encapsulation** command, described in the "Configuring Transponder Line Card Channel Frequency" section on page 5-6 to configure OFC on a transparent interface.

About Laser Safety Control

The Cisco ONS 15530 allows you to enable laser safety control on the trunk side interfaces of the transponder line cards. Much like OFC, the laser safety control protocol shuts down the transponder line card laser transmitting to the trunk when a fiber cut occurs or when the trunk fiber is detached from the shelf (see Figure 5-3).

Figure 5-3 Laser Safety Control Overview



Laser safety control uses the same protocol state machine as OFC, but not the same timing. Laser safety control uses the pulse interval and pulse duration timers compliant with the ALS (automatic laser shutdown) standard (ITU-T G.664).

Use laser safety control with line card protected and unprotected configurations only. Enable laser safety control on all wave interfaces, including the OSC.

Caution Laser safety control can interrupt signal transmission with splitter protected configurations. If you configure the system with splitter protection and enable laser safety control, the transmit laser to the client shuts down when an open fiber occurs on one transport fiber and signal transmission to the client is interrupted.

Configuring Laser Shutdown

This sections describes how to configure forward laser control and laser safety control on the Cisco ONS 15530 transponder line card interfaces.

Note To function correctly, configure forward laser control on both the transparent and wave interfaces on a transponder line card. For y-cable protection, forward laser control on both the transparent and wave interfaces on both transponder line cards will be configured automatically.

Configuring Forward Laser Control

To configure forward laser control for transparent and wave interfaces on a transponder line card, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface transparent** *slot*/*subcard*/*port* Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [**no**] **laser control forward enable**	Configures forward laser control on the interface. The default state is disabled.
Step 3	Switch(config-if)# **exit**	Returns to global configuration mode.
Step 4	Switch(config)# **interface wave** *slot*/*subcard* Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
Step 5	Switch(config-if)# [**no**] **laser control forward enable**	Configures forward laser control on the interface. The default state is disabled.

Caution Do not configure forward laser control when OFC is enabled. Combining these features interferes with the OFC protocol.

Examples

The following example shows how to configure forward laser control for the transparent and wave interfaces on a transponder line card:

```
Switch(config)# interface transparent 5/0/0
Switch(config-if)# laser control forward enable
Switch(config-if)# exit
Switch(config)# interface wave 5/0
Switch(config-if)# laser control forward enable
```

The following example shows how to configure forward laser control for an OSC wave interface:

```
Switch(config)# interface wave 0
Switch(config-if)# laser control forward enable
```

Displaying Forward Laser Control Configuration

To display the forward laser control configuration of a transparent or wave interface, use the following EXEC command:

Command	Purpose
show interfaces {**transparent** *slot*/*subcard*/*port* | **wave** *slot*/*subcard*}	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is administratively up, line protocol is up
  Encapsulation: Sonet    Rate: oc3
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change 10:18:20
➔ Forward laser control: On
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 10:18:20
  Hardware is transparent
```

Configuring Laser Safety Control

To configure laser safety control on a wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface wave** *slot*/*subcard*} Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [**no**] **laser control safety enable**	Enables or disables laser safety control.

Note Use laser safety control only with line card protected and unprotected configurations. Enable laser safety control on all the wave interfaces in the shelf, including the OSC.

Caution Do not configure laser safety control when OFC is enabled. Combining these features interferes with the OFC safety protocol.

Example

The following example shows how to configure laser safety control on a wave interface:

```
Switch(config)# interface wave 8/0
Switch(config-if)# laser control safety enable
```

Displaying Laser Safety Control Configuration

To display the laser safety control configuration of a wave interface, use the following EXEC command:

Command	Purpose
show interfaces wave *slot*/*subcard*	Displays interface information.

Example

The following example shows how to display the laser safety control configuration for an interface:

```
Switch# show interfaces wave 10/0
Wave10/0 is administratively up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz    Wavelength: 1536.61 nm
  Splitter Protected: Yes
  Receiver power level: -10.0 dBm
➔ Laser safety control: On
  Forward laser control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
```

Configuring Optical Power Thresholds

Optical power thresholds provide a means of monitoring the signal power from the ITU laser. Four types of thresholds are provided:

- Low alarm
- Low warning
- High warning
- High alarm

When a threshold is crossed, the system sends a message to the console.

Note The default values for the optical power receive thresholds are sufficient for most network configurations.

To configure optical power thresholds for wavepatch interfaces on a transponder line card, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface wavepatch** *slot*/*subcard*/*port* Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **optical threshold power receive {low** | **high**} **{alarm** | **warning**} *value* [**severity {critical** | **major** | **minor** | **not alarmed** | **not reported**}**]**	Specifies the optical power threshold value in units of 0.1 dBm. The default values on the active wavepatch are as follows: Low alarm: –28 dBm Low warning: –24 dBm High warning: –10 dBm High alarm: –8 dBm Alarm severity: **major** Warning severity: **not alarmed** The default values on the standby wavepatch are as follows: Low alarm: –28 dBm Low warning: –24 dBm High warning: –15 dBm High alarm: –13 dBm Alarm severity: **major** Warning severity: **not alarmed**

Examples

The following example shows how to configure optical power thresholds for wavepatch interfaces on a transponder line card:

```
Switch(config)# interface wavepatch 5/0/0
Switch(config-if)# laser control forward enable
```

Displaying Optical Power Threshold Configuration

To display the optical power thresholds for a wavepatch interface, use the following EXEC command:

Command	Purpose
show interfaces wavepatch *slot*/*subcard*/*port*	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces wavepatch 4/0/0
Wavepatch4/0/0 is up, line protocol is up
  Receiver power level: -23.91 dBm
  Optical threshold monitored for : Receive Power (in dBm)
  Low alarm value = -28.0  (default)
  Low Alarm Severity = major
  Low warning value = -24.0  (default)
  Low Warning Severity = not alarmed
  High alarm value = -8.0  (default)
  High Alarm Severity = major
  High warning value = -10.0  (default)
  High Warning Severity = not alarmed
  Hardware is passive_port
```

About Patch Connections

Because the OADM modules are passive devices, the Cisco ONS 15530 does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connection configuration using the CLI.

Table 5-3 describes the types of patch connections on the Cisco ONS 15530.

Table 5-3 Patch Connection Types

Patch Connection	Description
Thru interface to thru interface	Connection between two OADM modules in different chassis slots.
Wavepatch interface to filter interface or filter interface to wavepatch interface	Connection between the wavepatch on a 10-Gbps ITU trunk card and the filter interface on an OADM module.
OSC wave interface to oscfilter interface or oscfilter interface to OSC wave interface	Connection between the OSC wave interface and the oscfilter interface on the OADM module in the same chassis slot.

For more information on patch connection rules, see the *Cisco ONS 15530 Planning and Design Guide*.

Configuring Patch Connections

To configure patch connections between OADM modules within the same shelf, use the following global configuration commands:

Command	Purpose
patch thru *slot1*/*subcard1* **thru** *slot2*/*subcard2*	Configures the patch connection between two add/drop OADM modules in different chassis slots.
patch wavepatch *slot1*/*subcard1*/*port1* **filter** *slot2*/*subcard2*/*port2* or **patch filter** *slot1*/*subcard1*/*port1* **wavepatch** *slot2*/*subcard2*/*port2*	Configures the patch connection between a 10-GE trunk card and a OADM module.
patch wave *slot*/*subcard* **oscfilter** *slot*/*subcard* or **patch oscfilter** *slot*/*subcard* **wave** *slot*/*subcard*	Connection between the OSC wave interface and the oscfilter interface on the OADM module in the same chassis slot.

Note If you correctly patch your OADM modules, **patch** command configuration is not necessary for the signal to pass from the client to the trunk fiber. However, without correct **patch** command configuration, CDP is unable to locate the wdm interfaces that connect to the trunk fiber and discover the topology neighbors. For more information on network monitoring, see the "Configuring CDP" section on page 9-3.

Example

The following example shows how to configure the patch connections:

```
Switch# configure terminal
Switch(config)# patch thru 0/0 thru 0/1
Switch(config)# patch wave 0 oscfilter 0/0
Switch(config)# patch wave 1 oscfilter 0/1
Switch(config)# patch wavepatch 4/0/0 filter 0/0/1
Switch(config)# patch wavepatch 4/0/1 filter 0/1/1
```

Displaying Patch Connections

To display the patch connections, use the following privileged EXEC command:

Command	Purpose
show patch [**detail**]	Displays the patch connections.

Note The error field in the **show patch** command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a transponder line card and a OADM module, “Channel Mismatch” appears for the patch connection. When more than one OADM module drops the same channels, “Channel Mismatch” appears for all patch connections.

Example

The following example shows the patch connections:

```
Switch# show patch

Patch Interface    Patch Interface    Type    Error
---------------    ---------------    ----    -----
Thru0/0            Wdm0/1             USER
Thru0/1            Wdm0/2             USER
Thru0/2            Thru1/0            USER
Thru1/1            Wdm1/0             USER
Thru1/2            Wdm1/1             USER
Wave0              Oscfilter0/0       USER
Wave1              Oscfilter1/2       USER
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15530. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Displaying Cross Connections

To display the signal path cross connections, use the following privileged EXEC command:

Command	Purpose
show connect [**edge** | **intermediate** [**sort-channel** | **interface** {**transparent** *slot*/*subcard*/*port* | **wave** *slot*/*subcard*}]]	Displays the optical connections.

Examples

The following example shows the cross connections within a system configured for splitter protection:

```
Switch# show connect intermediate
client/       wave          wave           wdm
wave          client        patch   filter  trk  channel
------------  ------------  -------  ------  ---  -------
Trans2/0/0    Wave2/0        2/0/0*  0/0/0   0/0    1
                             2/0/1   1/0/0   1/0    1
Trans2/2/0    Wave2/2        2/2/0*  0/0/2   0/0    3
                             2/2/1   1/0/2   1/0    3
Trans2/3/0    Wave2/3        2/3/0*  0/0/3   0/0    4
                             2/3/1   1/0/3   1/0    4
```

The following example shows the cross connections within a system configured for line card protection using splitter protected line card motherboards:

```
Switch# show connect intermediate
client/       wave           wave            wdm
wave          client          patch   filter  trk  channel
------------  ------------  -------  ------  ---  -------
Trans10/0/0   Wave10/0      10/0/0*  0/3/0   0/2    25
                            10/0/1
Trans10/1/0   Wave10/1      10/1/0*  0/3/1   0/2    26
                            10/1/1
Trans10/2/0   Wave10/2      10/2/0*  0/3/2   0/2    27
                            10/2/1
Trans10/3/0   Wave10/3      10/3/0*  0/3/3   0/2    28
                            10/3/1
```

Configuring VOA Module Interfaces

This chapter describes how to configure the VOA modules supported by the Cisco ONS 15530. These modules allow the Cisco ONS 15530 to extend the internodal distances and number of nodes supported for point-to-point, hubbed ring, and meshed ring topology networks.

This chapter includes the following sections:

About Variable Optical Attenuation

The attenuation typically occurs on the input side of the EDFA (erbium-doped fiber amplifier) so that the input power of each band transmitted to the EDFA is equalized. The VOA modules can also attenuate OSC channels, EDFA output (when preamplifying), or individual data channels.

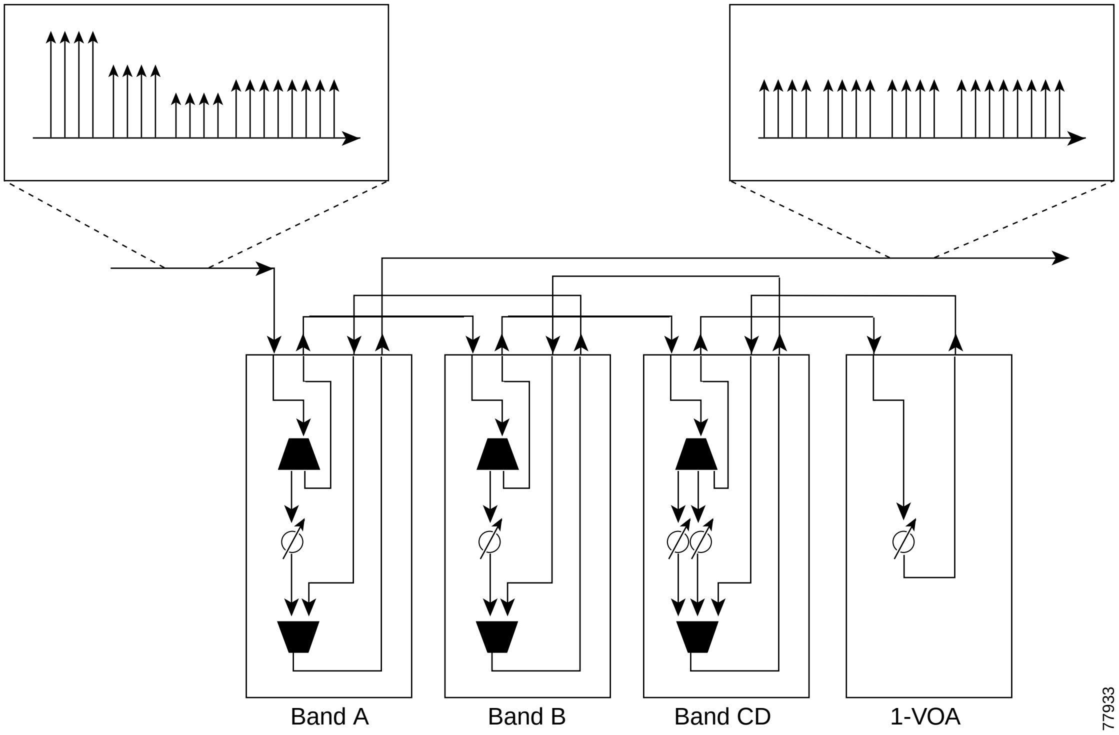
The Cisco ONS 15530 supports two types of VOA modules:

- PB-OE (per-band optical equalizer) modules
- WB-VOA (wide-band variable optical attenuator) modules

A PB-OE module selects one or two bands of channels to attenuate and passes on the rest of the signal. WB-VOA modules attenuate all the channels it receives.

Figure 6-1 illustrates the use of PB-OE and WB-VOA modules to perform band based power equalization.

Figure 6-1 Four Channel Equalization with Three Power Equalizers



VOA Modules

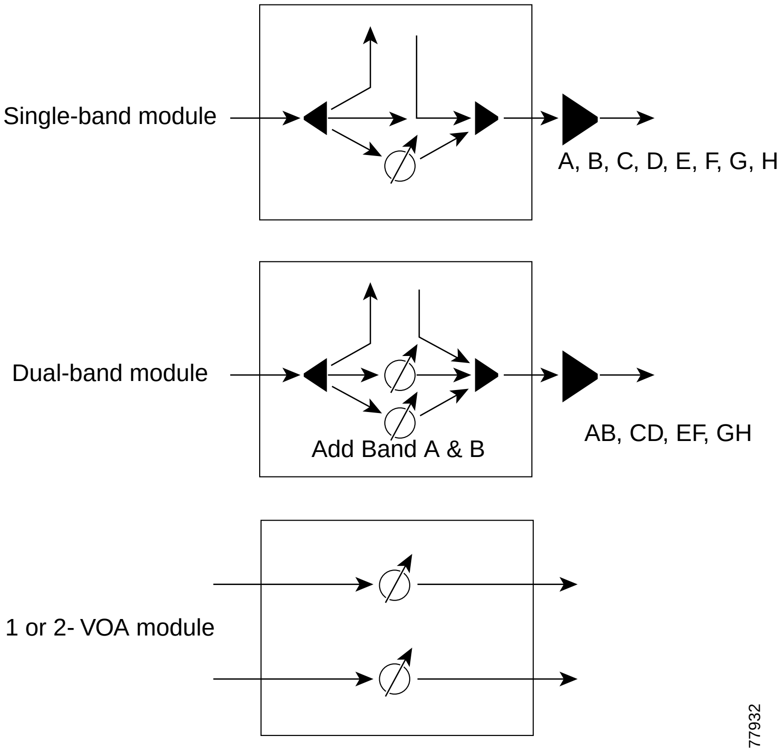
The VOA modules are half-width modules inserted into a carrier motherboard installed in a Cisco ONS 15530 shelf. The carrier motherboards can be installed in slots 1 through 4 and 7 through 10. All optical connectors are located on the front panel and the connectors are angled and recessed.

Each carrier motherboard can hold up to two VOA modules. There are four types of VOA modules available:

- Single WB-VOA modules
- Dual WB-VOA modules
- Single band PB-OE modules
- Dual band PB-OE modules

Figure 6-2 shows the types of VOA modules.

Figure 6-2 Types of VOA modules



Single WB-VOA Modules

The single WB-VOA modules accept one signal and attenuate all frequencies within that signal. The signal can contain a single channel, such as the OSC, a band of channels, or multiple channel bands.

Dual WB-VOA Modules

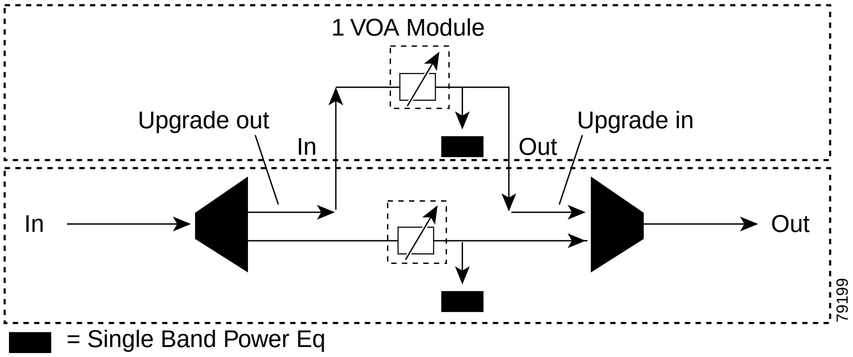
The dual WB-VOA modules consist of two WB-VOA units that each accepts one signal and attenuates all frequencies within that signal.

Single Band PB-OE Modules

A single band PB-OE module accepts an incoming signal containing at least two bands, which are split by an optical filter into two components. The first component is attenuated and the second component is passed to an another module where it can be attenuated and passed back to the original PB-OE. The PB-OE then recombines the two equalized components into a single signal and sends it out.

Figure 6-3 below shows enlarged views of a single band PB-OE and single WB-VOA module for pass band attenuation.

Figure 6-3 Single Band Power Equalizer

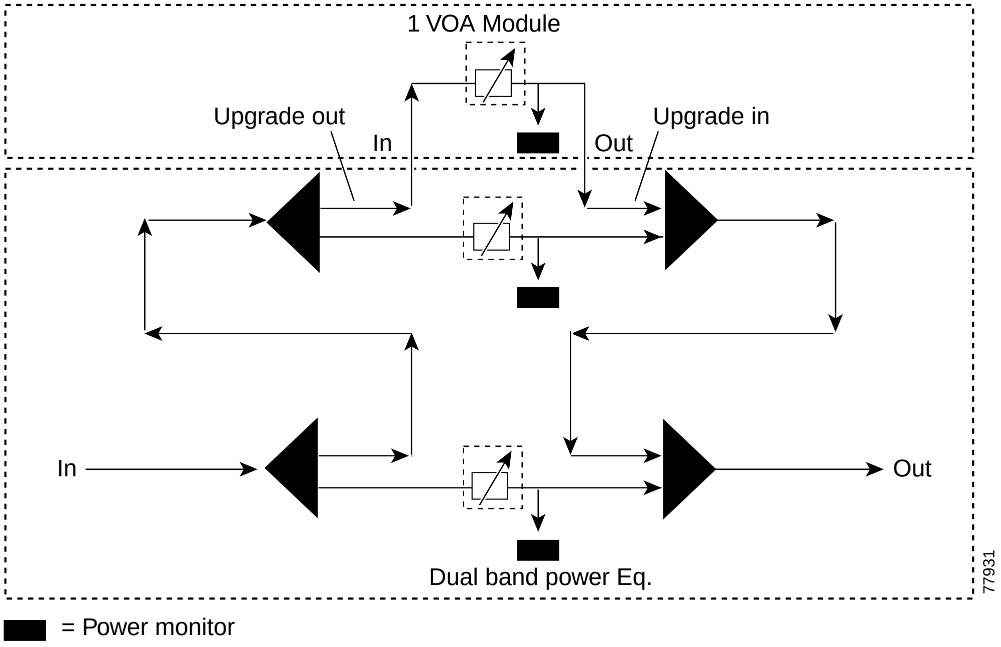


Dual Band PB-OE

If two consecutive bands have to be attenuated, use a dual band PB-OE module. When more than two add bands are to be attenuated, multiple VOA modules can be cascaded. The dual band PB-OE supports bands AB, CD, EF, and GH. Use a dual band PB-OE module to equalize signals with at least two bands.

The diagram below show enlarged views of a dual band PB-OE module and single WB-VOA module for pass band attenuation.

Figure 6-4 Dual Band Power Equalizer



Configuring VOA Module Interfaces

The following steps describe the configuration tasks for optical amplification support on the Cisco ONS 15530:

Step 1 Configure attenuation values (optional).

Step 2 Configure alarm thresholds (optional).

Configuring Attenuation

To configure the attenuation on a VOA module interface, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	Enter global configuration mode.
Step 2	Switch(config)# **interface** {**voafilterin** *slot*/*subcard*/*port***.***subinterface* | **voain** *slot*/*subcard*/*port*} Switch(config-if)#	Selects the VOA interface to configure and enters interface configuration mode.
Step 3	Switch(config-if)# **optical attenuation manual** *value*	Specifies the value in units of 0.1 dBm.

Example

The following example shows how to configure attenuation on a voafilterin subinterface on a PB-OE module:

```
Switch# configure terminal
Switch(config)# interface voafilterin 1/0/0.1
Switch(config-subif)# optical attenuation manual 20
```

The following example shows how to configure attenuation on a voain interface on a WB-VOA module:

```
Switch# configure terminal
Switch(config)# interface voain 1/0/0
Switch(config-if)# optical attenuation manual 30
```

Displaying the Attenuation Configuration

To verify the configuration of attenuation configuration, use the following EXEC command:

Command	Purpose
show interfaces {**voafilterin** *slot*/*subcard*/*port***.***subinterface* | **voain** *slot*/*subcard*/*port*}	Displays the VOA module interface configuration.

Example

The following example shows how to display the attenuation configuration of a voafilterin subinterface:

```
Switch# show interfaces voafilterin 2/1/0.2
voaFilterIn2/1/0.2 is up, line protocol is up
  Hardware is voaFilterIn Port
  Port Transmit (Tx) Support:      False
  Port Receive  (Rx) Support:      True
  VOA This Port operates on:       1
  Minimum settable Attenuation:    3.7dB
  Maximum settable Attenuation:    30.0dB
➔ Current set Attenuation:         20.0dB
  Light Quality:                   Low Warning Threshold Exceeded
  Current Output Power:            -16.3dBm
  Low Alarm Threshold:             -20.0dBm
  Low Alarm Threshold Severity:    major (Default Value)
  Low Warning Threshold:           -15.0dBm
  Low Warning Threshold Severity:  not-alarm (Default Value)
  High Warning Threshold:          -10.0dBm
  High Warning Threshold Severity: not-alarm (Default Value)
  High Alarm Threshold:            -5.0dBm
  High Alarm Threshold Severity:   major (Default Value)
```

The following example shows how to display the attenuation configuration of a voain interface:

```
Switch# show interfaces voain 7/1/0
voaIn7/1/0 is up, line protocol is down
  Hardware is voaIn Port
  Port Transmit (Tx) Support:      False
  Port Receive  (Rx) Support:      True
  VOA This Port operates on:       1
  Minimum settable Attenuation:    1.7dB
  Maximum settable Attenuation:    30.0dB
➔ Current set Attenuation:         1.7dB
  Light Quality:                   Loss of Light/Low Alarm Threshold Exceeded
  Current Output Power:            -256.0dBm
  Low Alarm Threshold:             -29.0dBm (Default Value)
  Low Alarm Threshold Severity:    major (Default Value)
  Low Warning Threshold:           -20.0dBm
  Low Warning Threshold Severity:  not-alarm (Default Value)
  High Warning Threshold:          -5.0dBm
  High Warning Threshold Severity: not-alarm (Default Value)
  High Alarm Threshold:            0.0dBm
  High Alarm Threshold Severity:   major (Default Value)
```

About Optical Thresholds

You can configure optical thresholds on the VOA module interfaces that issue alarm messages to the system if the optical thresholds are exceeded. Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

Configuring Optical Receive Power Thresholds

TheVOA modules have optical receive power thresholds monitored by the Cisco ONS 15530 chassis. This section describes four types of alarm threshold configuration procedures:

- Low Power Alarm
- Low Power Warning
- High Power Warning
- High Power Alarm

Low power warnings are raised when the received optical power drifts too close to LOL (loss of light). Low power alarms show a critical condition of LOL. High power warnings are raised when the received optical power drifts too close to high power alarm conditions. High power alarm are raised when received optical power exceeds the receiver saturation threshold.

To configure power thresholds on VOA module interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface** {**voafilterin** *slot*/*subcard*/*port***.***subinterface* | **voain** *slot*/*subcard*/*port*}	Selects the VOA interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **optical threshold power receive after-attenuation** {**low** | **high**} {**alarm** | **warning**} *value* [**severity** {**critical** | **major** | **minor** | **not alarmed** | **not reported**}]	Specifies the threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: –29 dBm Low warning: –27 dBm High warning: 9 dBm High alarm: 11 dBm Alarm severity: **major** Warning severity: **not alarmed**

Displaying the Optical Threshold Configuration

To display the configuration of an optical threshold for a VOA interface, use the following EXEC commands:

Command	Purpose
show interfaces {**voafilterin** *slot*/*subcard*/*port***.***subinterface* | **voain** *slot*/*subcard*/*port*}	Displays the VOA module interface configuration.

Example

The following example shows how to display the threshold configuration of a voafilterin subinterface:

```
Switch# show interfaces voafilterin 2/1/0.2
voaFilterIn2/1/0.2 is up, line protocol is up
  Hardware is voaFilterIn Port
  Port Transmit (Tx) Support:      False
  Port Receive  (Rx) Support:      True
  VOA This Port operates on:       1
  Minimum settable Attenuation:    3.7dB
  Maximum settable Attenuation:    30.0dB
  Current set Attenuation:         20.0dB
  Light Quality:                   Low Warning Threshold Exceeded
  Current Output Power:            -16.3dBm
  Low Alarm Threshold:             -20.0dBm
  Low Alarm Threshold Severity:    major (Default Value)
  Low Warning Threshold:           -15.0dBm
  Low Warning Threshold Severity:  not-alarm (Default Value)
  High Warning Threshold:          -10.0dBm
  High Warning Threshold Severity: not-alarm (Default Value)
  High Alarm Threshold:            -5.0dBm
  High Alarm Threshold Severity:   major (Default Value)
```

The following example shows how to display the threshold configuration of a voain interface:

```
Switch# show interfaces voain 7/1/0
voaIn7/1/0 is up, line protocol is down
  Hardware is voaIn Port
  Port Transmit (Tx) Support:      False
  Port Receive  (Rx) Support:      True
  VOA This Port operates on:       1
  Minimum settable Attenuation:    1.7dB
  Maximum settable Attenuation:    30.0dB
  Current set Attenuation:         1.7dB
  Light Quality:                   Loss of Light/Low Alarm Threshold Exceeded
  Current Output Power:            -256.0dBm
  Low Alarm Threshold:             -29.0dBm (Default Value)
  Low Alarm Threshold Severity:    major (Default Value)
  Low Warning Threshold:           -20.0dBm
  Low Warning Threshold Severity:  not-alarm (Default Value)
  High Warning Threshold:          -5.0dBm
  High Warning Threshold Severity: not-alarm (Default Value)
  High Alarm Threshold:            0.0dBm
  High Alarm Threshold Severity:   major (Default Value)
```

Configuring APS

This chapter describes how protection is implemented on the Cisco ONS 15530. It also describes how to configure splitter protection and line card protection with APS (Automatic Protection Switching).This chapter contains the following sections:

About APS

APS provides protection against signal transmission failure. The Cisco ONS 15530 supports the following APS features:

- 1+1 path protection
- Splitter protection
- Line card protection
  - Client based
  - Y-cable based
  - Switch fabric based

- Redundant switch fabric protection
- Bidirectional and unidirectional path switching

The 1+1 path protection acrhitecture transmits the client signal on both the working and protection paths.

Note For an animated description of the APS implementation on the Cisco ONS 15530, go to the following URL:

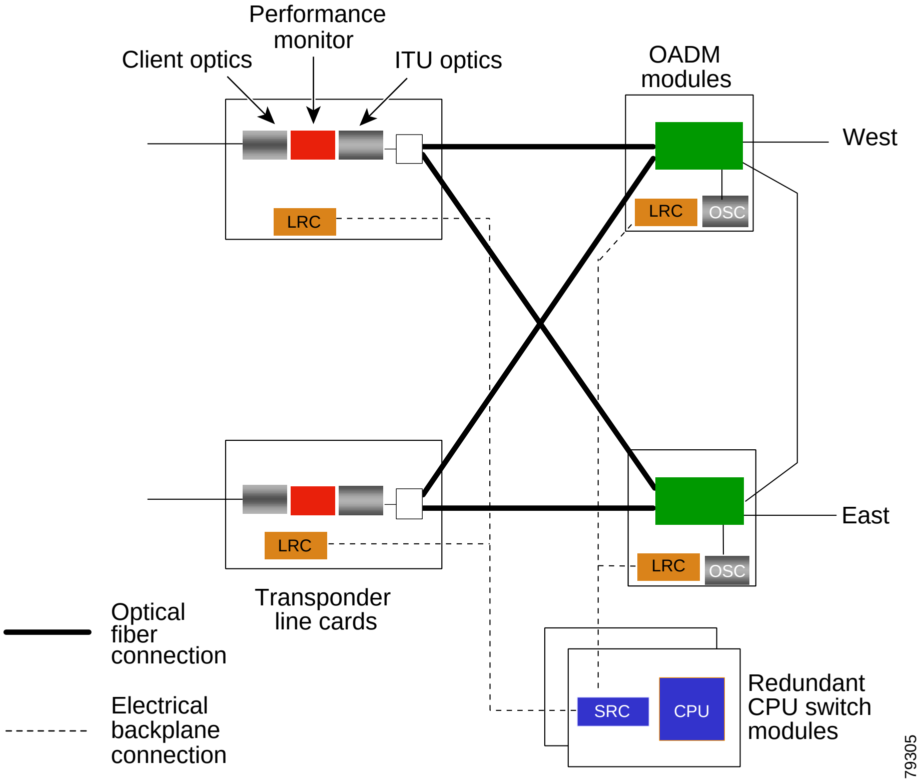
http://www.cisco.com/mm/dyngraph/APS15530.html

About Splitter Protection

Splitter protection on the Cisco ONS 15530 provides protection against facility failure, such as trunk fiber cuts, but not ITU laser failures or client equipment failures. Splitter line cards internally replicate the client optical signal and transmit it to both OADM modules. The Cisco ONS 15530 support s splitter versions of the transponder line card and the 10-Gbps ITU trunk card.

Figure 7-1 shows splitter protection with a transponder line card.

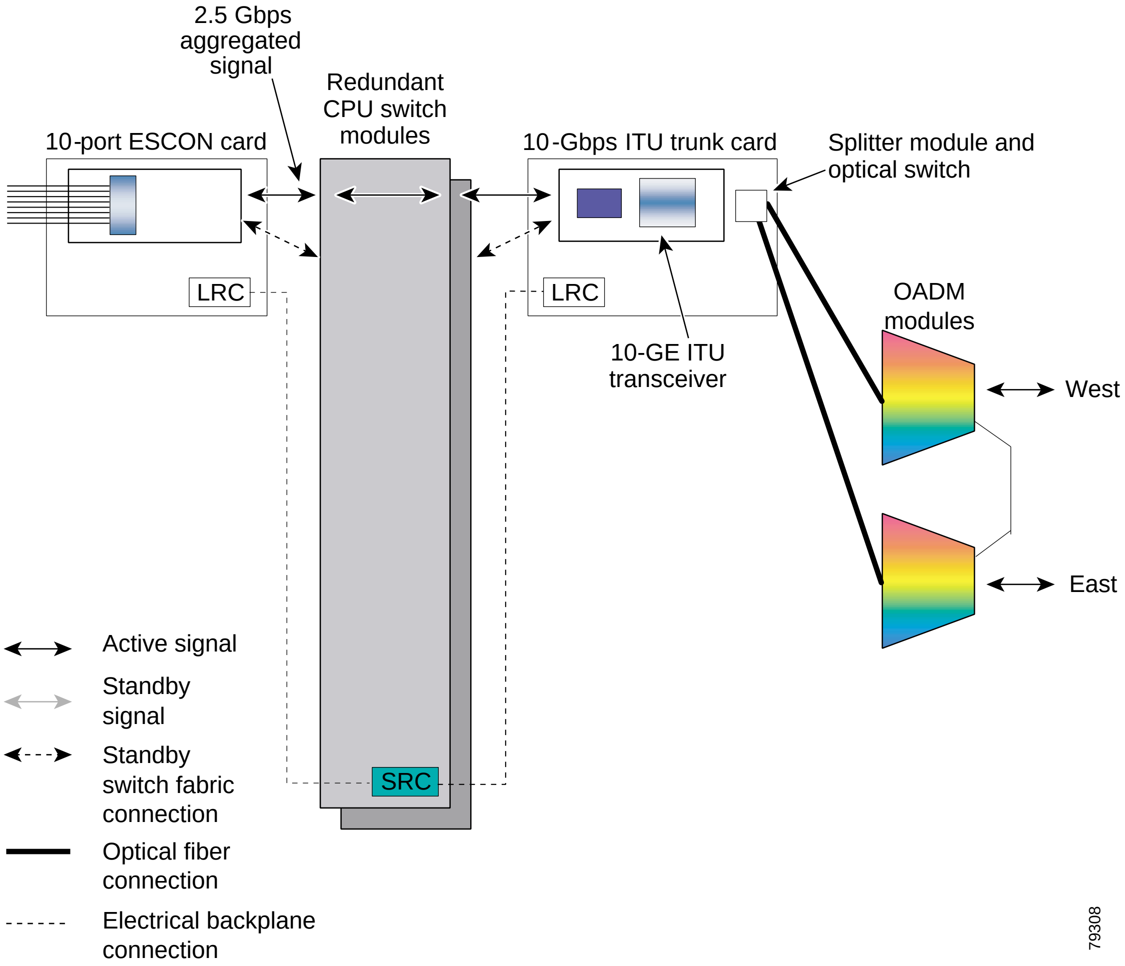
Figure 7-1 Splitter Protection Scheme



On the ITU side, a fiber pair, with one receive fiber and one transmit fiber, connects to the OADM module transmitting in the west direction. Another fiber pair connects to the OADM module transmitting in the east direction. A 2x2 switch module on the line card receives both signals from the trunk fiber pairs and selects one as the active signal. When a signal failure is detected, the line card switches over to receive the standby signal. The standby signal then becomes the active signal.

Figure 7-2 shows splitter protection with a 10-Gbps ITU trunk card.

Figure 7-2 Cisco ONS 15530 Trunk Card Splitter Protection


2.5 Gbps aggregated signal
Redundant CPU switch modules
10-port ESCON card
10-Gbps ITU trunk card
Splitter module and optical switch
LRC
LRC
OADM modules
10-GE ITU transceiver
West
East
SRC
Active signal
Standby signal
Standby switch fabric connection
Optical fiber connection
Electrical backplane connection
79308

Considerations for Using Splitter Protection

The following considerations apply when considering the use of splitter protection:

- Splitter protection does not protect against failure of the splitter line card. Splitter protection also does not protect against failure of a client line card or of the client equipment.

  To protect against laser failure for both transponder line cards and 10-Gbps ITU trunk cards, use y-cable protection as described in the "About Line Card Protection" section on page 7-6 and the "Configuring Y-Cable Based Line Card Protection" section on page 7-10. To protect against ESCON card failure or the client equipment, implement protection on the client equipment instead.
- A fully provisioned single shelf configuration can support 4 channels in splitter protection mode. A fully provisioned multiple shelf configuration can support up to 32 channels in splitter protection mode.

  For more information about multiple shelf nodes, see Chapter 8, "Configuring Multiple Shelf Nodes."
- Splitter protection supports revertive behavior. With revertive APS, the signal automatically switches back to the working path after the receive signal defect has been corrected and the wait to restore timer is expired. The default behavior is nonrevertive. When defects on the working channel are cleared, a wait to restore timer is started. Once this timer expires, the working channel becomes the active channel if no other problems occur on the working path.
- For interfaces configured for splitter APS and either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of these protocols.
- For bidirectional path switching to function on the transponder line cards, the OSC is required for exchanging APS channel protocol messages. For bidirectional path switching on the 10-Gbps ITU trunk card, either the in-band message channel or the OSC can be used for the APS channel protocol messages.

For detailed information on shelf configuration rules, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Configuring Splitter Protection

The following steps describe the tasks required to configure splitter protection:

Step 1 Determine the number of channels you will deploy to transport client data.

Step 2 Ensure that the correct line cards are inserted in slots 1 through 4 or 7 through 10.

Step 3 Ensure that the line cards and modules are correctly interconnected with the external optical patch cables. For ring topologies, connect the thru interface on one OADM to the thru interface on the other.

Step 4 Configure the interfaces and the patch connections from the CLI (command-line interface).

Step 5 Configure APS from the CLI.

Caution Do not enable laser safety control with splitter protection. If you configure the system with splitter protection and enable laser safety control, the transmit laser shuts down when an open fiber occurs on one transport fiber and signal transmission to the client is interrupted.

To configure splitter protection, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps working wavepatch** *slot*/*subcard*/*port*	Configures the working path interface.
Step 4	Switch(config-red-aps)# **aps protection wavepatch** *slot*/*subcard*/*port*	Configures the protection path interface.
Step 5	Switch(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

Examples

This example shows how to associate wavepatch interfaces for the transponder line card in slot 3 for splitter protection and modify the default attribute settings.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group dallas1
Switch(config-red-aps)# aps working wavepatch 3/0/0
Switch(config-red-aps)# aps protection wavepatch 3/0/1
Switch(config-red-aps)# aps enable
```

Displaying the Splitter Protection Configuration

To display the splitter protection configuration, use the following EXEC commands:

Command	Purpose
show aps	Displays the APS configuration summary.
show aps {**detail** | **group** *name* | **interface wavepatch** *slot*/*subcard*/*port*}	Displays detailed APS configuration information for groups and interfaces. **Note** Group names are case sensitive.

Example

The following example shows how to display the APS splitter protection configuration:

```
Switch# show aps

AR : APS Role, Wk: Working, Pr: Protection
AS : APS State, Ac: Active, St: Standby, NA: Not Applicable
IS : Interface State, Up: Up, Dn: Down
MPL: Minimum Protection Level, SD: Signal Degrade, SF: Signal Failure
     LOL: Loss of Light, - not currently protected

Interface             AR AS IS MPL Redundant Intf        Group Name
~~~~~~~~~~~~~~~~~~~~~ ~~ ~~ ~~ ~~~ ~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~~~~~~~
Wavepatch8/0/0        Wk Ac Up LOL Wavepatch8/0/1        Seattle
Wavepatch8/0/1        Pr St Up -   Wavepatch8/0/0        Seattle

Switch# show aps group Seattle

APS Group Seattle :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: network side splitter
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: yes, wtr: 60 secs (not running)
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 0 minutes
  auto-failover: enabled
  transmit k1k2: no-request, 0, 0, 1+1, uni
  receive  k1k2: no-request, 0, 0, 1+1, uni
  switched chan: 0
  protection(0): Wavepatch8/0/1 (STANDBY - UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
  working...(1): Wavepatch8/0/0 (ACTIVE - UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

About Line Card Protection

Line card protection on the Cisco ONS 15530 provides protection against both facility failures and line card failures. With line card protection, a duplicated signal is transmitted over ITU channels generated on separate line cards.

The Cisco ONS 15530 supports three types of line card protection:

- Client based protection
- Y-cable protection
- Switch fabric based protection

About Client Based Line Card Protection

In client protection mode, both signals are transmitted to the client system. The client system decides which signal to use and when to switch over.

Note Client protection does not require APS configuration on the Cisco ONS 15530.

Figure 7-3 shows an example of line card protection using transponder line cards.

Figure 7-3 Client Based Line Card Protection Using Transponder Line Cards

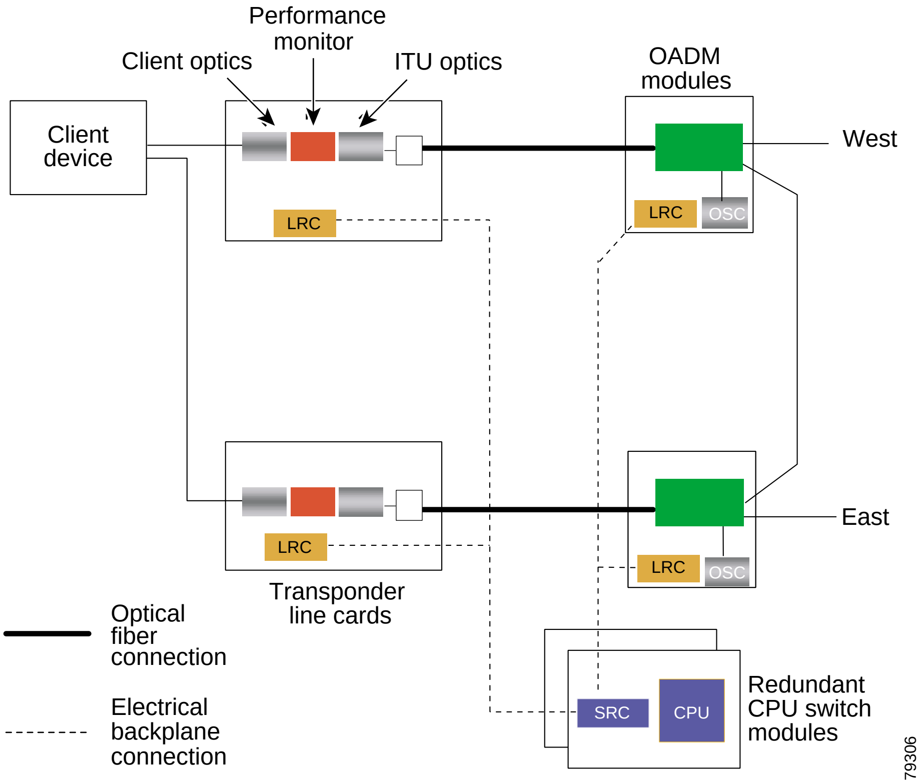
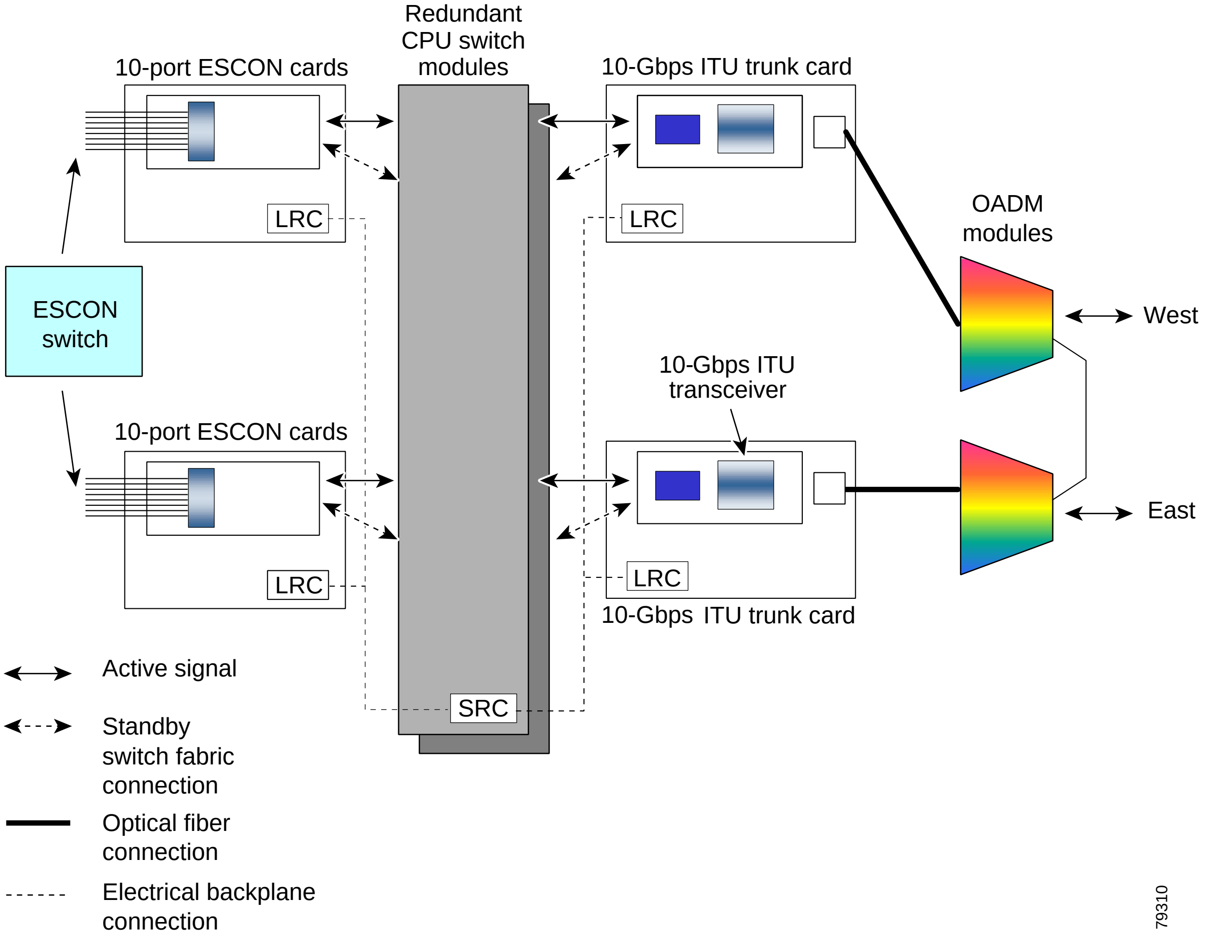


Figure 7-4 shows an example of line card protection using ESCON multiplexing line cards and 10-Gbps ITU trunk cards.

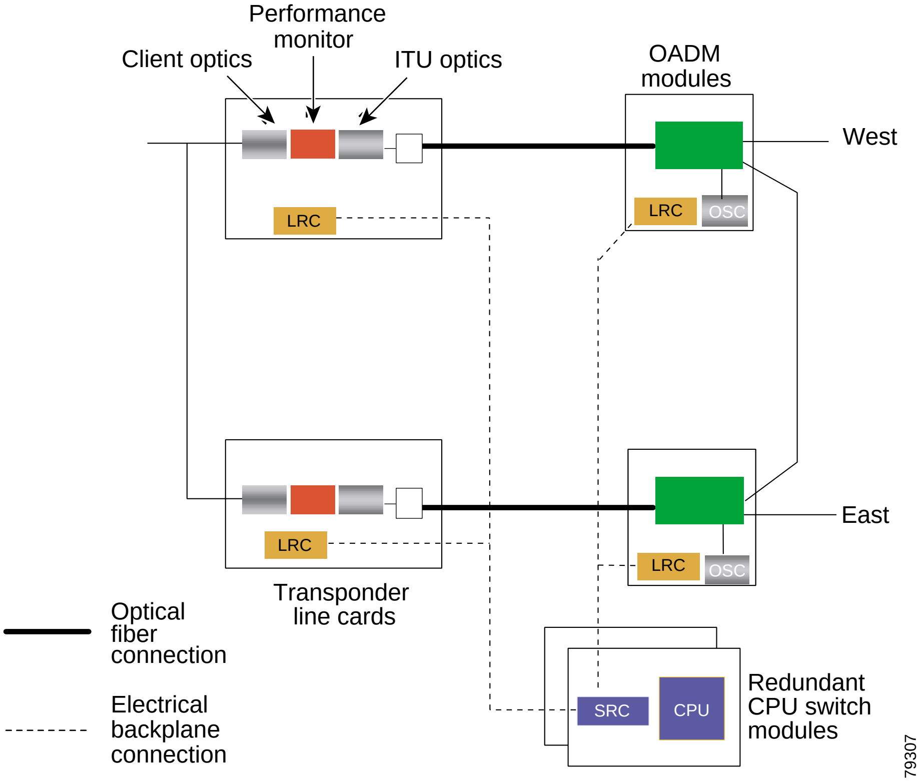
Figure 7-4 Client Based Line Card Protection Using ESCON Multiplexing Line Cards and 10-Gbps ITU Trunk Cards



About Y-Cable Line Card Protection

With y-cable protection, the client equipment sends only one signal to two transponder line cards using a y-cable to replicate the signal. The client equipment receives from only one transponder line card. The Cisco ONS 15530 turns on the laser at the active transparent interface, and turns off the laser on the standby transparent interface. At each receiver on the trunk side of the transponder line card, the system monitors the optical signal power level. If the system detects a failure of the active signal when an acceptable signal exists on the standby transponder line card, a switchover to the standby signal occurs by turning off the active transmitter at the client interface and turning on the standby transmitter.

Figure 7-5 Y-Cable Based Line Card Protection Scheme



Considerations for Using Y-Cable Based Line Card Protection

The following considerations apply when considering the use of line card protection:

- Y-cable line card protection does not protect against failures of the client equipment. To protect against client failures, ensure that protection is implemented on the client equipment itself.
- A fully provisioned single shelf configuration can support up to 4 channels with line card protection using transponder line cards. A fully provisioned multiple shelf configuration can support up to 32 channels in line card protection mode.

  For more information about multiple shelf nodes, see Chapter 8, "Configuring Multiple Shelf Nodes."
- Y-cable line card protection supports revertive behavior. With revertive behavior, the signal automatically switches back to the working path after the signal failure has been corrected. The default behavior is nonrevertive.
- To simplify system management, terminate the client signal on line cards that support the same channel. In this way the client signal maps to the same WDM wavelength on both the working and protection paths.

Caution Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Proper physical configuration of the system is critical to the operation of line card protection. For detailed information on shelf configuration rules, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Configuring Y-Cable Based Line Card Protection

The following is an overview of the tasks required to configure line card protection:

Step 1 Determine the number of clients you need to support and which channels you will deploy to transport the client data.

Step 2 Ensure that the OADM modules needed to support the deployed channels are installed in the shelf. (See the "Considerations for Using Y-Cable Based Line Card Protection" section on page 7-9.)

Step 3 Ensure that the OADM modules are correctly interconnected with the external optical patch cables.

Step 4 In order to ensure separate paths to the OADM modules, shut down the unused wavepatch interfaces if you are using splitter line cards.

Step 5 Configure the interfaces and the patch connections from the CLI.

Step 6 Configure y-cable protection from the CLI.

Y-cable protection on the Cisco ONS 15530 requires configuration on the CLI. To configure y-cable protection, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps working transparent** *slot*/*subcard*/*port*	Configures the working path interface.
Step 4	Switch(config-red-aps)# **aps protection transparent** *slot*/*subcard*/*port*	Configures the protection path interface.
Step 5	Switch(config-red-aps)# **aps y-cable**	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 6	Switch(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

⚠ **Caution** Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Example

This example shows how to associate two transparent interfaces for y-cable line card protection.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group Yosemite
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# end
Switch#
```

Displaying the Y-Cable Protection Configuration

To display the y-cable protection configuration, use the following EXEC command:

Command	Purpose
show aps	Displays the APS configuration summary.
show aps {**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/*port*}}	Displays detailed APS configuration information for interfaces and groups. **Note** Group names are case sensitive.

Example

The following example shows how to display the y-cable protection for an APS group:

```
Switch# show aps

AR : APS Role, Wk: Working, Pr: Protection
AS : APS State, Ac: Active, St: Standby, NA: Not Applicable
IS : Interface State, Up: Up, Dn: Down
MPL: Minimum Protection Level, SD: Signal Degrade, SF: Signal Failure
     LOL: Loss of Light, - not currently protected

Interface             AR AS IS MPL Redundant Intf        Group Name
~~~~~~~~~~~~~~~~~~~~~ ~~ ~~ ~~ ~~~ ~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~~~~~~
Transparent4/0/0      Wk St Up -   Transparent7/0/0      Yosemite
Transparent7/0/0      Pr Ac Up SD  Transparent4/0/0      Yosemite

Switch# show aps group Yosemite

APS Group Yosemite :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: client side y-cable
  direction....: prov: bi, current: bi, remote prov: bi
  revertive....: no
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 17 hours, 10 minutes
  auto-failover: enabled
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive  k1k2: forced-switch, 1, 1, 1+1, bi
  switched chan: 1
```

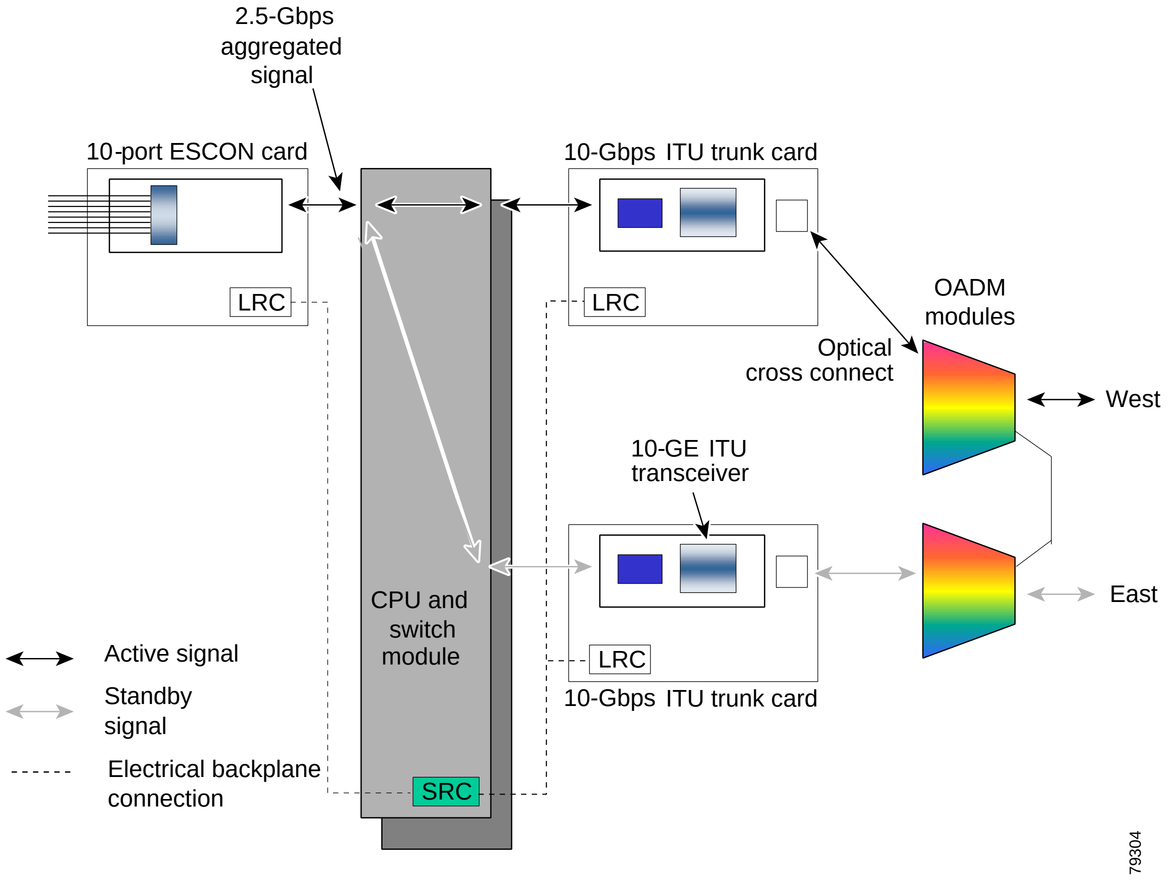
```
protection(0): Transparent7/0/0 (ACTIVE - UP), Wave7/0 (UP)
             : channel  request: no-request
             : switchover count: 2
             : last  switchover: 15 hours, 14 minutes
working...(1): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
             : channel  request: no-request
             : switchover count: 3
             : last  switchover: 14 hours, 41 minutes
```

About Switch Fabric Based Line Card Protection

The Cisco ONS 15530 provides protection for cross connections through the switch fabric. Switch fabric based line card protection is supported on systems with one or two switch fabrics.

The aggregated signals from the multiplexing line cards cross connect through the switch fabric to either a 10-Gbps ITU trunk card or to a 10-GE uplink card. In switch fabric based line card protection, the system sets up a protection cross connection through the switch fabric to a second 10-Gbps ITU trunk card or a 10-GE uplink card (see Figure 7-6).

Figure 7-6 Switch Fabric Based Line Card Protection with Redundant Switch Fabrics



Switch fabric based line card protection protects against facility failures and failures in 10-Gbps ITU trunk cards and 10-GE uplink cards.

Note Splitter protection and y-cable protection cannot be configured with switch fabric based protection.

Considerations for Using Switch Fabric Based Line Card Protection

The following considerations apply when considering the use of line card protection:

- Switch fabric based line card protection does not protect against failures of the client equipment or the ESCON multiplexing line card. To protect against such failures, use client based line card protection.
- A fully provisioned single shelf configuration can support up to two channels with switch fabric based line card protection. A fully provisioned multiple shelf configuration can support up to 32 channels in switch fabric based line card protection mode.

  For more information about multiple shelf nodes, see Chapter 8, "Configuring Multiple Shelf Nodes."
- Switch fabric based line card protection supports revertive behavior. With revertive behavior, the signal automatically switches back to the working path after the signal failure has been corrected. The default behavior is nonrevertive.
- To simplify system management, terminate the client signal on line cards of the same channel. In this way the client signal maps to the same WDM wavelength on both the working and protection paths.
- Configure unique flow identifiers on the ESCON multiplexing line card interfaces. Duplicate flow identifiers interfere with switchovers between line cards.
- Be sure that the subinterface on the protection line card does not have a configured cross connection. Such cross connection interfere with switchovers.

Proper physical configuration of the system is critical to the operation of switch fabric based line card protection. For detailed information on shelf configuration rules, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Configuring Switch Fabric Based Line Card Protection

To configure switch fabric based line card protection, use the following commands:

	Command	Purpose
Step 1	Switch# **show connect**	Displays the cross connect configuration.
Step 2	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 3	Switch(config)# **connect** {**waveethernetphy** | **tengigethernetphy**} *slot/subcard***.***subinterface* **portgroup** *slot/subcard/port* [**override**]	Configures cross connections on the line card.
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.

	Command	Purpose
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps working** {**waveethernetphy** | **tengigethernetphy**} *slot*/*subcard*	Configures the working path interface. ⚠ **Caution** Configuring the working path on the standby cross connection might cause a switchover. Configure the working path on the active cross connection to prevent such switchovers when the APS group is enabled.
Step 4	Switch(config-red-aps)# **aps protection** {**waveethernetphy** | **tengigethernetphy**} *slot*/*subcard*	Configures the protection path interface.
Step 5	Switch(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

Note When configuring the esconphy interfaces, use unique flow identifiers for each esconphy interface on the system. For more information on configuring esconphy interfaces, see the "Configuring ESCON Multiplexing Line Card Interfaces" section on page 4-2.

Note You can configure cross connections on either the working or the protection 10-Gbps ITU trunk cards or 10-GE uplink cards.

Displaying Switch Fabric Based Protection Configuration

To display the switch fabric based protection configuration, use the following EXEC command:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**waveethernetphy** | **tengigethernetphy**} *slot*/*subcard*]	Displays the APS configuration.

Example

The following example shows how to display the switch fabric based line card protection:

```
Switch# show aps detail

APS Group yellow :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: switch fabric based line card protection
  direction....: prov: bi, current: bi, remote prov: bi
  revertive....: no
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto-select (up on cdl dcc)
  created......: 0 minutes
  auto-failover: enabled
  transmit k1k2: no-request, 0, 0, 1+1, bi
  receive  k1k2: no-request, 0, 0, 1+1, bi
  switched chan: 0
  protection(0): WaveEthernetPhy8/0 (STANDBY - UP), xc DORMANT
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
  working...(1): WaveEthernetPhy7/0 (ACTIVE - UP), xc UP
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

About Redundant Switch Fabric Protection

The Cisco ONS 15530 provides protection for the 2.5-Gbps aggregated signals sent through the redundant switch fabrics.

Configuring APS Group Attributes

This section describes APS group attributes and how to configure them.

Configuring Revertive Switching

The Cisco ONS 15530 supports revertive switching for all types of protection. When revertive switching is configured, the system automatically switches back from the protection interface to the working interface. This automatic switchover occurs after the condition that caused the switchover to the protection interface is resolved and the switchover-enable timer has expired.

To configure revertive switching, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps disable**	Disables APS activity between the interfaces.
Step 4	Switch(config-red-aps)# **aps timer wait-to-restore** *seconds*	Modifies the interval for the wait-to-restore timer. If revertive protection is configured and a switchover has occurred, the system will wait this amount of time before switching back to the functioning working path. The default value is 300 seconds. (Optional)
Step 5	Switch(config-red-aps)# **aps revertive**	Enables revertive switchover behavior. The default behavior is nonrevertive.
Step 6	Switch(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

Displaying the Revertive Switching Configuration

To display the revertive switching configuration, use the following EXEC command:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/**0** | **gigethernetphy** *slot*/*subcard*/**0**}]	Displays the APS configuration for interfaces and groups. **Note** Group names are case sensitive.

Example

The following example shows how to display the path switching configuration for an APS group named blue:

```
Switch# show aps group blue

APS Group blue:

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: client side y-cable
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: yes, wtr: 300 secs (not running)
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 4 days, 23 hours, 16 minutes
  auto-failover: enabled
  transmit k1k2: no-request, 0, 0, 1+1, uni
  receive  k1k2: no-request, 0, 0, 1+1, uni
  switched chan: 0
  protection(0): Transparent7/0/0 (STANDBY - UP), Wave7/0 (UP)
               : channel  request: no-request
               : switchover count: 2
               : last  switchover: 3 days, 23 hours, 16 minutes
  working...(1): Transparent4/0/0 (ACTIVE - UP), Wave4/0 (UP)
               : channel  request: no-request
               : switchover count: 1
               : last  switchover: 4 days, 53 minutes
```

About Unidirectional and Bidirectional Path Switching

The Cisco ONS 15530 supports per-channel unidirectional and bidirectional 1+1 path switching. When a signal is protected and the signal fails or degrades on the active path, the system automatically switches the APS group from the active network path to the standby network path.

Signal failures can be total LOL (loss of light) caused by laser failures, by fiber cuts between the Cisco ONS 15530 and the client equipment, between two Cisco ONS 15530s, or by other equipment failures. LOL failures on the transponder line cards and LOLK (loss of lock) on the 10-Gbps ITU trunk cards and 10-GE uplink cards cause switchovers for protected signals.

For y-cable APS, you can also configure alarm thresholds to cause a switchover when the error rate detected on the signal reaches an unacceptable level. For information about configuring alarm thresholds, see the "Configuring Alarm Thresholds" section on page 4-13.

The Cisco ONS 15530 implements path switching using a SONET-compliant APS channel protocol over the in-band message channel or the OSC (optical supervisory channel).

Note Bidirectional path switching operates only on networks that support the OSC or the in-band message channel.

Figure 7-7 shows a simple point-to-point configuration with splitter protection. The configured working path carries the active signal, and the configured protection path carries the standby signal.

Figure 7-7 Active and Standby Path Configuration Example

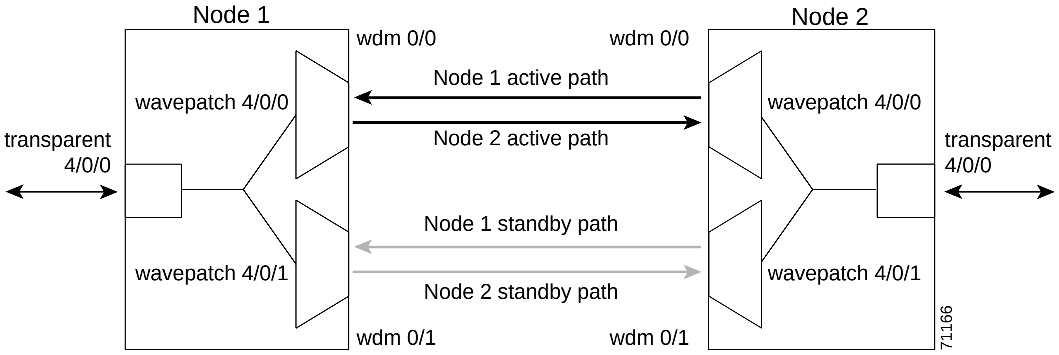


Figure 7-8 shows the behavior of unidirectional path switching when a loss of signal occurs. In the two node example network, unidirectional path switching operates as follows:

- Node 2 sends the signal over both the active and standby paths.
- Node 1 receives both signals and selects the signal on the active path.
- Node 1 detects a loss of signal light on its active path and switches over to the standby path.
- Node 2 does not switch over and continues to receive its original active path.

Now the nodes are communicating along different paths.

Figure 7-8 Unidirectional Path Switching Example

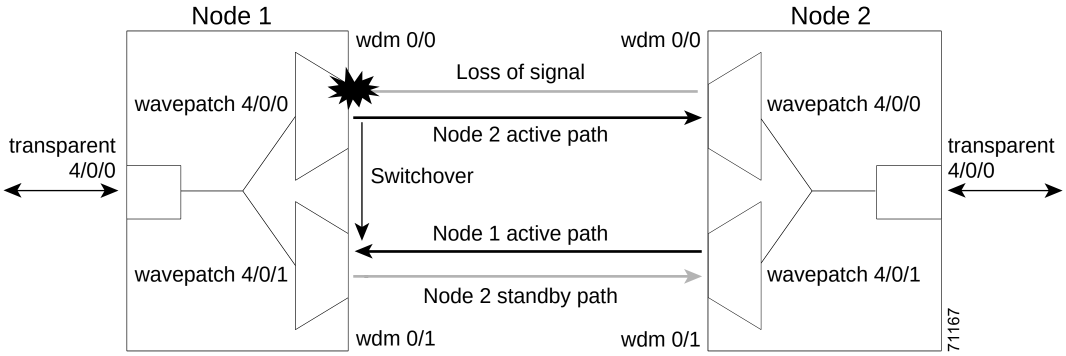
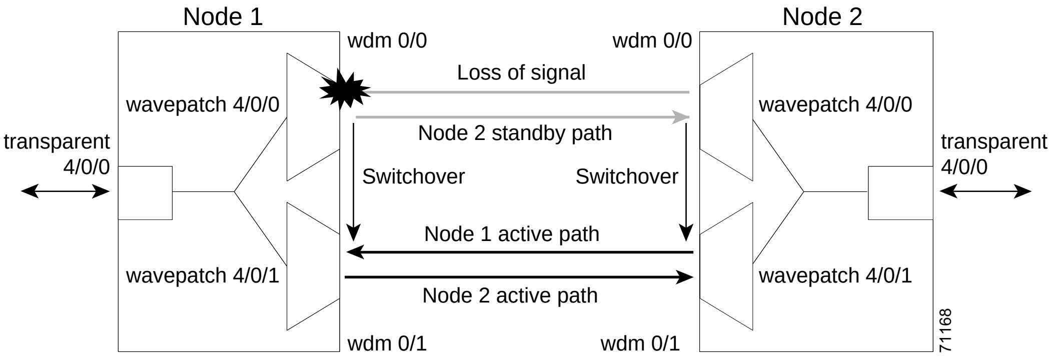


Figure 7-9 shows the behavior of bidirectional path switching when a loss of signal occurs. In the two node example network, bidirectional path switching operates as follows:

- Node 2 sends the signal over both the active and standby paths.
- Node 1 receives both signals and selects the signal on the active path.
- Node 1 detects a loss of signal light on its active path and switches over to the standby path.
- Node 1 sends an APS message to node 2 on the protection path indicating that it has switched.
- Node 2 processes the APS message and switches from the active path to the standby path.

Both node 1 and node 2 communicate on the same path.

Figure 7-9 Bidirectional Path Switching Overview



Configuring Unidirectional and Bidirectional Path Switching

To configure unidirectional or bidirectional path switching, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps disable**	Disables APS activity between the interfaces.
Step 4	Switch(config-red-aps)# **aps direction** {**unidirectional** | **bidirectional**}	Specifies the type of path switching. The default behavior is unidirectional.
Step 5	Switch(config-red-aps)# **aps timer message holddown** *milliseconds* **count** *number*	Changes the APS Channel Protocol holddown timer and message count values. The default is 5000 milliseconds and a count of 2. (Optional)

	Command	Purpose
Step 6	Switch(config-red-aps)# **aps timer message max-interval** *seconds*	Changes the APS Channel Protocol maximum interval timer for waiting for a message. The default is 15 seconds. (Optional) Repeat Step 1 through Step 6 on the corresponding transparent interface on the other node that adds and drops, or terminates, the channel.
Step 7	Switch(config-red-aps)# **aps message-channel** {**auto-select** [**far-end group-name** *name*] | **inband dcc** [**far-end group-name** *name*] | **ip far-end group-name** *name* **ip-address** *ip-address* | **osc** [**far-end group-name** *name*]}	Configures the message channel for the APS channel protocol messages. The default is **auto-select** without a group name. (Optional)
Step 8	Switch(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

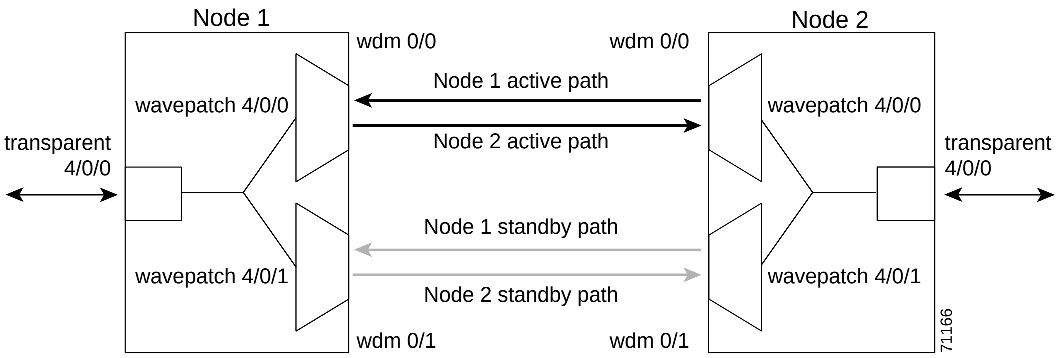
Note Both nodes in the network that add and drop the channel must have the same APS configuration. Specifically, both must have the same path switching behavior, and working and protection paths.

Note For interfaces with either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of the protocol.

Examples

Figure 7-10 shows the active and standby paths between node 1 and node 2 with splitter protection.

Figure 7-10 Bidirectional Path Switching Example with Splitter Protection



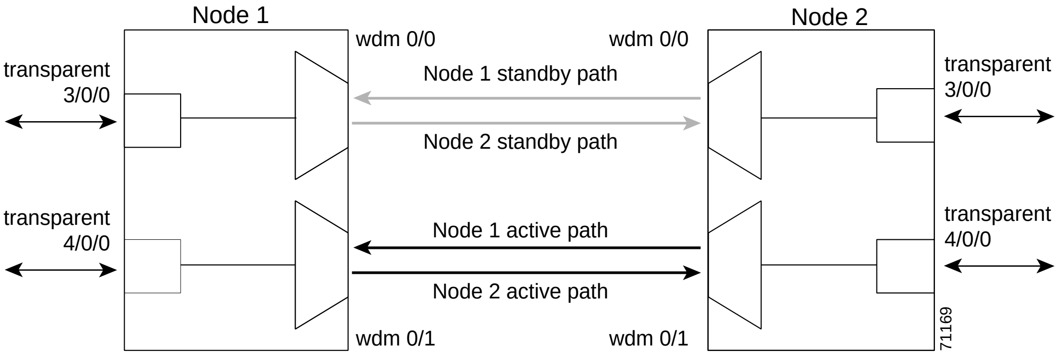
The following example shows how to configure one channel in the example network for bidirectional path switching using the default working and protection path interfaces:

```
Node1# configure terminal
Node1(config)# redundancy
Node1(config-red)# associate group red
Node1(config-red-aps)# aps working wavepatch 4/0/0
Node1(config-red-aps)# aps protection wavepatch 4/0/1
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps enable

Node2# configure terminal
```

```
Node2(config)# redundancy
Node2(config-red)# associate group red
Node2(config-red-aps)# aps working wavepatch 4/0/0
Node2(config-red-aps)# aps protection wavepatch 4/0/1
Node2(config-red-aps)# aps bidirectional
Node2(config-red-aps)# aps enable
```

Figure 7-11 shows the active and standby paths between node 1 and node 2 with y-cable protection.

Figure 7-11 Bidirectional Path Switching Example with Y-Cable Protection



The following example shows how to configure one channel in the example network for bidirectional path switching and configure the working and protection path interfaces:

```
Node1# configure terminal
Node1(config)# redundancy
Node1(config-red)# associate group alpha
Node1(config-red-aps)# aps working transparent 4/0/0
Node1(config-red-aps)# aps protection transparent 3/0/0
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable

Node2# configure terminal
Node2(config)# redundancy
Node2(config-red)# associate group alpha
Node2(config-red-aps)# aps working transparent 4/0/0
Node2(config-red-aps)# aps protection transparent 3/0/0
Node2(config-red-aps)# aps direction bidirectional
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps enable
```

Displaying the Unidirectional and Bidirectional Path Switching Configuration

To display the path switching configuration, use the following EXEC command:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/**0** | **gigethernetphy** *slot*/*subcard*/**0**}]	Displays the APS configuration for interfaces and groups. **Note** Group names are case sensitive.

Example

The following example shows how to display the path switching configuration for an APS group named blue:

```
Switch# show aps group blue

APS Group blue:

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
➔ direction....: prov: bi, current: bi, remote prov: bi
  revertive....: no
➔ msg-channel..: auto (up on osc)
  created......: 26 minutes
  aps state....: associated
➔ request timer: holddown: 5000 ms, max: 15 secs, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive  k1k2: forced-switch, 1, 1, 1+1, bi
  switched chan: 0
  channel  ( 0): Wavepatch8/0/1 (STANDBY - UP)
               : channel  request: no-request
               : transmit request: no-request
               : receive  request: no-request
  channel  ( 1): Wavepatch8/0/0 (ACTIVE - UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

Configuring the Switchover-Enable Timer

The switchover-enable timer on the Cisco ONS 15530 prevents any automatic switchover from the protection path to the working path until it has expired. When it expires, switchovers occur only if there is no fault on the working path and there is no overriding switchover request in effect.

To configure the switchover-enable timer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps disable**	Disables the APS group.
Step 4	Switch(config-red-aps)# **aps timer switchover-enable min-interval** *seconds*	Modifies the timer that controls the check on the status of the working path. The default is 2 seconds.
Step 5	Switch(config-red-aps)# **aps enable**	Enables the APS group.

Displaying the Switchover-Enable Timer Configuration

To display the switchover-enable timer configuration, use the following EXEC command:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/**0** | **gigethernetphy** *slot*/*subcard*/**0**}]	Displays the APS configuration for interfaces and groups. **Note** Group names are case sensitive.

Example

The following example shows how to display the path switching configuration for an APS group named blue:

```
Switch# show aps group blue

APS Group blue:

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  direction....: prov: bi, current: bi, remote prov: bi
  revertive....: yes
  msg-channel..: auto (up on osc)
  created......: 26 minutes
  aps state....: associated
  request timer: holddown: 5000 ms, max: 15 secs, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive  k1k2: forced-switch, 1, 1, 1+1, bi
  switched chan: 0
  channel   ( 0): Wavepatch8/0/1 (STANDBY - UP)
              : channel  request: no-request
              : transmit request: no-request
              : receive  request: no-request
  channel   ( 1): Wavepatch8/0/0 (ACTIVE - UP)
              : channel  request: no-request
              : switchover count: 0
              : last  switchover: never
```

About Switchovers and Lockouts

In APS, you can switch a channel signal from one path to another, or you can lock out a switchover altogether while performing system maintenance.

A switchover of the channel signal from the working path to protection path is useful when upgrading or maintaining the system, or in cases where a signal failure caused a switchover. The switchover to the formerly failed interface must be requested from the CLI. The interface originally configured as the working path might be preferred because of its link loss characteristics or because of its distance advantage. For example, some protocols, such as ESCON, experience lower data throughput at increasing distances, so moving the signal back to the shorter path might be advised.

A lockout prevents a switchover of the active signal from the working path to the protection path. This is useful when upgrading or maintaining the system, or repairing the protection path when it degrades or fails.

The Cisco ONS 15530 supports APS switchover and lockout requests from the CLI. These requests have priorities depending on the condition of the protection signal and the existence of other switchover requests. There are three types of switchover requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the active signal from switching over from the working path to the protection path.
- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the protection path, or the signal on the protection path has failed when switching from working to protection.
- Manual switchover requests—Have the lowest priority and are only honored if there is no lockout, forced switchover, or signal failure or degrade.

In summary, the priority order is:

1. Lockout
2. Signal failure on the protection path
3. Forced switchover
4. Signal failure on the working path
5. Signal degrade on the protection path
6. Signal degrade on the working path
7. Manual switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

Note APS lockouts and forced or manual switchover requests do not persist across processor card switchovers or system reloads.

Requesting a Switchover or Lockout

To prevent switchovers to the protection signal, or to request a signal switchover, use the following commands in privileged EXEC mode:

Command	Purpose
aps lockout *group-name*	Locks out all switchovers to the protection path.
aps switch *group-name* {**force** | **manual**} {**protection-to-working** | **working-to-protection**}	Requests a signal switchover of the active signal from the working path to the protection path, or vice versa, within an associated interface pair.

Examples

The following example shows how to request a forced switchover from working to protection except if a lockout is in effect on the protection path:

```
Switch# aps switch blue force working-to-protection
```

The following example shows how to prevent a switchover to the protection path:

```
Switch# aps lockout blue
```

Displaying Switchover and Lockout Request Status

To display a pending switchover request, use the following command in privileged EXEC mode:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* **| waveethernetphy** *slot/subcard*}]	Displays the APS configuration for interfaces and groups. **Note** Group names are case sensitive.

The following example shows how to display the switchover request status on an APS group:

```
Switch# show aps group blue

APS Group yellow:

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (client side y-cable)
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  msg-channel..: auto (up on osc)
  created......: 15 hours, 1 minute
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive  k1k2: forced-switch, 1, 1, 1+1, bi
  switched chan: 0
  channel  ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
➔              : channel  request: lockout-of-protection
➔              : transmit request: lockout-of-protection
               : receive  request: no-request
  channel  ( 1): Transparent2/0/0 (ACTIVE - UP), Wave2/0 (UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

Clearing Switchovers and Lockouts

A lockout stays in effect until the system reboots. A forced or manual switchover request stays in effect until the system reboots or a higher priority request preempts it. You can manually clear these requests from the CLI.

To clear an APS switchover or lockout request, use the following privileged EXEC command:

Command	Purpose
aps clear *group-name*	Clears APS switch request or lockout on an associated interface pair.

Example

The following example shows how to clear the requests on an associated interface pair using the default group name:

```
Switch# aps clear blue
```

Displaying Switchover and Lockout Clear Status

To display a pending switchover request, use the following command in privileged EXEC mode:

Command	Purpose
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/**0** | **gigethernetphy** *slot*/*subcard*/**0**}]	Displays the APS configuration for interfaces and groups. **Note** Group names are case sensitive.

The following example shows how to display the lockout and switchover request status on an APS group:

```
Switch# show aps group blue

APS Group blue :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (client side y-cable)
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  msg-channel..: auto (up on osc)
  created......: 15 hours, 1 minute
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive  k1k2: forced-switch, 1, 1, 1+1, bi
  switched chan: 0
  channel  ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
➔              : channel  request: lockout-of-protection
➔              : transmit request: lockout-of-protection
               : receive  request: no-request
  channel  ( 1): Transparent2/0/0 (ACTIVE - UP), Wave2/0 (UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

CHAPTER 8

Configuring Multiple Shelf Nodes

This chapter describes how to configure a multiple shelf node in a network topology. This chapter contains the following sections:

- About Multiple Shelf Nodes, page 8-1
- Configuring Multiple Shelf Nodes, page 8-1

About Multiple Shelf Nodes

On a single Cisco ONS 15530 shelf, only 4 channels can be supported. By cascading multiple Cisco ONS 15530 shelves, up to 32 channels can be supported. You can use multiple shelf nodes in either a point-to-point topology or a ring topology. The OSCs (optical supervisory channels) can both connect to one shelf, or they can be split between the two shelves.

Configuring Multiple Shelf Nodes

To configure a multiple shelf node, follow these steps:

Step 1 Populate the shelves with the motherboards, cards, and processor cards.

Step 2 Connect the OADM modules with cables and configure the patch connections.

Step 3 Configure the client interfaces.

Step 4 Establish network access to both shelves.

For information on configuring network access, see the "Configuring IP Access on the NME Interface" section on page 3-3.

Step 5 Configure IP addresses on the OSC wave interfaces.

For information on configuring IP address on the OSC wave interface, see the "Configuring IP on the OSC" section on page 9-9.

Step 6 Configure the network topology information for the connections between the two shelves.

Step 7 Configure APS (Automatic Protection Switching) on the shelves in the network that support the channels.

Configuring Patch Connections Between Shelves

To represent the three shelves as one node in the network topology, you must configure the patch connection between the shelves in the CLI (command-line interface). To configure these connections, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# **interface** {**wave** *slot* | **oscfilter** *slot*/*subcard* | **thru** *slot*/*subcard* | **wdm** *slot*/*subcard*}	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **topology neighbor** {**name** *node-name* | **ip-address** *node-ip-address* | **mac-address** *node-mac-address*} {**port** {**name** *port-name* | **ip-address** *port-ip-address* | **mac-address** *port-mac-address*}}	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# **topology neighbor agent ip-address** *ip-address*	Specifies the address of the network topology agent on a neighboring node.

Note Configure the patch connections between the OADM modules on the same shelf as described in the "Configuring Patch Connections" section on page 4-15.

Examples

The following example shows how to configure the patch connections between the OADM modules on the three shelves in the example node:

```
Shelf1(config)# interface wdm 0/0
Shelf1(config-if)# topology neighbor name node1 port name wdm 0/1
Shelf1(config-if)# topology neighbor agent ip-address 10.1.1.1
Shelf1(config-if)# exit
Shelf1(config)# interface thru 0/0
Shelf1(config-if)# topology neighbor name shelf2 port name wdm 0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf1(config-if)# exit
Shelf1(config)# interface wdm 0/1
Shelf1(config-if)# topology neighbor name shelf2 port name thru 0/1
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf1(config-if)# exit
Shelf1(config)# interface thru 0/1
Shelf1(config-if)# topology neighbor name shelf3 port name thru 0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf1(config-if)# exit
```

```
Shelf2(config)# interface wdm 0/0
Shelf2(config-if)# topology neighbor name shelf1 port name thru 0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf2(config-if)# exit
Shelf2(config)# interface thru 0/0
Shelf2(config-if)# topology neighbor name shelf3 port name wdm 0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf2(config-if)# exit
Shelf2(config)# interface wdm 0/1
Shelf2(config-if)# topology neighbor name shelf3 port name thru 0/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf2(config-if)# exit
Shelf2(config)# interface thru 0/1
Shelf2(config-if)# topology neighbor name shelf1 port name wdm 0/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf2(config-if)# exit

Shelf3(config)# interface wdm 0/0
Shelf3(config-if)# topology neighbor name Shelf2 port name thru 0/0
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf3(config-if)# exit
Shelf3(config)# interface thru 0/0
Shelf3(config-if)# topology neighbor name shelf1 port name thru 0/1
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf3(config-if)# exit
Shelf3(config)# interface wdm 0/1
Shelf3(config-if)# topology neighbor name Node3 port name thru 0/0
Shelf3(config-if)# topology neighbor agent ip-address 10.3.3.1
Shelf3(config-if)# exit
Shelf3(config)# interface thru 0/1
Shelf3(config-if)# topology neighbor name shelf2 port name wdm 0/1
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf3(config-if)# exit
```

Configuring APS

When a multiple shelf node is part of a network topology, the channels supported by it might require special configuration. On a multiple shelf node, the OSC might have only one connection or no OSC connections at all. For the APS channel protocol to function correctly, the shelves that support a channel must both have two OSC connections, or you must configure the APS group name and IP address information on the shelves.

To configure APS for a channel supported on a multiple shelf node without full OSC support, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# **redundancy** Switch1(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# **associate group** *name* Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. **Note** The group name is case sensitive.
Step 3	Switch(config-red-aps)# **aps disable**	Disables APS activity between the interfaces. **Note** For newly created APS groups, APS activity is disabled by default.

	Command	Purpose
Step 4	Switch(config-red-aps)# **aps working wavepatch** *slot*/*subcard*/*port*	Configures the working path interface.
Step 5	Switch(config-red-aps)# **aps protection wavepatch** *slot*/*subcard*/*port*	Configures the protection path interface.
Step 6	Switch1(config-red-aps)# **aps y-cable**	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 7	Switch1(config-red-aps)# **aps message-channel ip far-end group** *group-name* **ip-address** *address*	Configures the APS group name and IP address on the remote node that supports the channel.
Step 8	Switch1(config-red-aps)# **aps enable**	Enables APS activity between the interfaces.

For more information on configuring y-cable line card protection, refer to the "Configuring Y-Cable Based Line Card Protection" section on page 7-10.

Examples

For these examples, assume the following:

- Channels 17–20 terminate on the second shelf of the multiple shelf node.
- The second shelf of the multiple shelf node has no OSC support.
- The management IP address of the second shelf of the multiple shelf node is 10.1.2.3.
- The management IP address of the single shelf node is 10.3.2.1.

The following example shows how to configure channels 17–20 on the single shelf node:

```
Switch(config)# redundancy
Switch(config-red)# associate group Channel17
Switch(config-red-aps)# aps working transparent 1/0/0
Switch(config-red-aps)# aps protection transparent 2/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel17 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel18
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel18 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel19
Switch(config-red-aps)# aps working transparent 7/0/0
Switch(config-red-aps)# aps protection transparent 8/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel19 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel20
Switch(config-red-aps)# aps working transparent 9/0/0
Switch(config-red-aps)# aps protection transparent 10/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel20 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# end

Switch# copy system:running-config nvram:startup-config
```

The following example shows how to configure channels 17–20 on shelf 2 of a multiple shelf node.

```
Shelf3(config)# redundancy
Shelf3(config-red)# associate group Channel17
Shelf3(config-red-aps)# aps working transparent 1/0/0
Shelf3(config-red-aps)# aps protection transparent 2/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel17 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel18
Shelf3(config-red-aps)# aps working transparent 3/0/0
Shelf3(config-red-aps)# aps protection transparent 4/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel18 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel19
Shelf3(config-red-aps)# aps working transparent 7/0/0
Shelf3(config-red-aps)# aps protection transparent 8/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel19 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel20
Shelf3(config-red-aps)# aps working transparent 9/0/0
Shelf3(config-red-aps)# aps protection transparent 10/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel20 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# end

Shelf3# copy system:running-config nvram:startup-config
```

Monitoring Your Network Topology

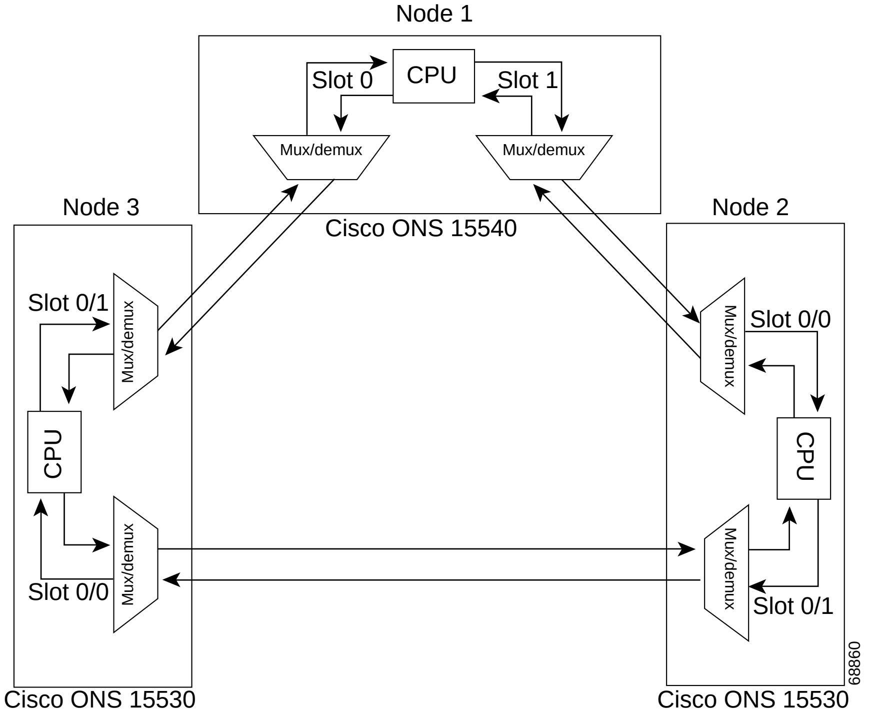
This chapter describes how to configure and manage your network topology. This chapter includes the following sections:

About the OSC

As described in the "OSC Modules" section on page 1-5, the Cisco ONS 15530 dedicates a separate channel (channel 0) for the OSC (optical supervisory channel), which is used for network control and management information between Cisco ONS 15530 systems on the network. The OSC is carried on the same fiber as the data channels (channels 1 through 32), but it carries no client data traffic.

Figure 9-1 shows the path of the OSC in a protected ring configuration. The OSC signal is generated by a laser on an OSC card and is sent in both directions from the node; both receive signals are monitored to maintain communication with the neighboring nodes. The OSC signal terminates at each node.

Figure 9-1 OSC Signal Path in a Ring Configuration



The OSC performs the following functions:

- Discovery—CDP (Cisco Discovery Protocol) sends packets on the OSC to discover neighboring nodes. CDP runs by default every 60 seconds. The information gathered by CDP can be displayed using the CLI (command-line interface) and used by the NMS (network management system) to discover the logical topology of the network.
- Monitoring—OSCP (OSC Protocol) runs over the OSC to provide monitoring of the status of adjacent nodes. OSCP is a keepalive mechanism similar to the PNNI Hello protocol used in ATM (Asynchronous Transfer Mode). Using OSCP, nodes exchange packets that allow them to determine the operational status of their neighbors. OSCP must establish that there is two-way communication before declaring to the upper layer protocols that a node is "up."
- Management—IP packets are carried over the OSC to support SNMP and Telnet sessions. Using Telnet over the OSC allows you to access the CLI of all systems on your Cisco ONS 15530 network with a single Ethernet connection. Also, just one Ethernet connection is required from the NMS to monitor all Cisco ONS 15530 systems on the network using SNMP.

Hardware Guidelines for Using OSC

To provide protection against failure of the laser or a fiber break in protected configurations (point-to-point or ring), the following rules apply:

- One slot contains a carrier motherboard with two OSC cards.
- Both OADM modules must support OSC along with the band of wavelengths.

For more information on hardware configuration rules, refer to the
Cisco ONS 15530 Planning and Design Guide.

Configuring CDP

CDP is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. For a full description of CDP and details on configuring the protocol, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*. For a full description of the CDP commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

On the Cisco ONS 15530, you can configure CDP at both the global level and the interface level. The global-level CDP configuration sets the attributes for the entire system. The interface-level configuration identifies interfaces connected to the client equipment and to the trunk interface to CDP. Because there are only optical connections to the client equipment, you must explicitly identify the transparent interfaces connected to the client equipment. On wdm interfaces, you can choose to provide the information about the interface in the CLI or you can let CDP discover it.

Note The shelf must include the OSC to support CDP. If the OSC is not present, see the "Monitoring Without the OSC or In-Band Message Channel" section on page 9-19.

Configuring Global CDP

To configure CDP on your Cisco ONS 15530, use the following commands in global configuration mode:

Command	Purpose
cdp advertise-v2	Specifies CDP version 2 advertisements. The default is version 2.
cdp holdtime *seconds*	Specifies the amount of time the receiving device should hold a CDP packet from the sending device before discarding it. The default value is 180 seconds.
cdp timer *seconds*	Specifies how often to send CDP updates. The default value is 60 seconds.
[no] cdp run	Enables and disables CDP on the device. The default state is enabled.

Examples

In the following example, the CDP packets being sent from your device should be held by the receiving device for 60 seconds before being discarded:

```
Switch(config)# cdp holdtime 60
```

In the following example, CDP updates are sent every 80 seconds:

```
Switch(config)# cdp timer 80
```

Displaying the Global CDP Configuration

To display the configured CDP values, use the following EXEC command:

Command	Purpose
show cdp	Displays the configured CDP timer, holdtime, and advertisement settings.

Example

The following example shows how to display the configured CDP values:

```
Switch> show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
```

Displaying Global CDP Information

You can display information gathered by CDP, including a specific neighbor device listed in the CDP table, the interfaces on which CDP is enabled, and the traffic between devices gathered using CDP.

To display the CDP information, use the following EXEC commands:

Command	Purpose
show cdp entry {***** | *entry-name*} [**protocol** | **version**]	Displays information about all neighbors or a specific neighbor discovered by CDP. Optionally, displays the protocol and version.
show cdp interface [*type number*]	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays a list of CDP neighbors.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

Example

The following example shows how to display CDP status and activity information:

```
Switch1# show cdp entry *
-------------------------
Device ID: Switch2
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco ,  Capabilities: Router
Interface: Wave2/0,  Port ID (outgoing port): Wave2/0
Holdtime : 176 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) ONS-15530 Software (manopt-I-M), Experimental Version 12.1 [koj-ons 122]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 12:04 by koj
advertisement version: 2
```

```
Switch1# show cdp interface
Wave2/0 is up, line protocol is up
  Encapsulation UNKNOWN
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Switch1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch2          Wave2/0              158          R                  Wave2/0

Switch1# show cdp traffic
CDP counters :
        Total packets output: 18, Input: 20
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 18, Input: 20
```

Clearing Global CDP Information

You can reset the CDP traffic counters to zero and clear the table that contains the CDP neighbor information. To clear the CDP information, use the following privileged EXEC commands:

Command	Purpose
clear cdp counters	Resets the CDP traffic counters to zero.
clear cdp table	Clears the table that contains the CDP neighbor information.

Configuring CDP Topology Discovery on Wdm Interfaces

You can enable CDP topology discovery on the wdm interfaces that connect to the trunk fiber. CDP then automatically advertises interface information to neighboring nodes.

Note The Cisco ONS 15530 enables CDP topology discovery by default on the wdm interfaces connecting to the trunk fiber.

To configure CDP topology discovery on wdm interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **topology hold-time** *seconds*	Modifies the interval to hold a nonstatic network topology node entry. The default value is 300 seconds.
Step 2	Switch(config)# **interface wdm** *slot*/*subcard* Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 3	Switch(config-if)# **topology neighbor cdp [proxy** *interface*] or Switch(config-if)# **topology neighbor disable**	Enables CDP topology discovery on the interface. The default is enabled. or Disables CDP on the interface.

Examples

The following example shows how to enable CDP topology discovery on a wdm interface:

```
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor cdp
```

The following example shows how to disable CDP topology discovery on a wdm interface:

```
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor disable
```

Displaying CDP Information for Wdm Interfaces

You can display interface-level information gathered by CDP, including neighboring devices.

To display the CDP information for an interface, use the following EXEC commands:

Command	Purpose
show topology neighbor [**detail**]	Displays information about the physical network topology neighbors for the node.
show topology	Displays the global physical network topology configuration.

Example

```
Switch# show topology neighbor

Physical Topology:

Local Port    Neighbor Node      Neighbor Port
----------    -------------      -------------
Wd0/0         Node1              wdm1/1
Wd0/1         Node2              wdm0/2
Trans8/0/0    Router1            gigabitethernet1/1

Switch# show topology
Global Physical Topology configuration:
  Maximum Hold Time = 300 secs
 Trap interval = 60 secs
```

Configuring OSCP

The configurable parameters of the OSCP are described in the following sections.

Note The default values are suitable in most cases.

Configuring the Hello Interval Timer

The OSCP sends Hello packets to adjacent nodes at a configured interval. When five packets fail to get a response from the receiving node, that node is declared "down." By decreasing the interval at which Hello packets are sent, reaction time to a failed node can be lessened. Increasing the interval reduces the amount of Hello packet traffic.

To configure the OSCP Hello timer interval, use the following global configuration command:

Command	Purpose
oscp timer hello interval *milliseconds*	Configures the Hello interval timer in milliseconds. The default value is 100 milliseconds.

Example

The following example shows how to set the Hello interval to 500 milliseconds:

```
Switch(config)# oscp timer hello interval 500
```

Configuring the Hello Hold-Down Timer

The Hello hold-down timer specifies the interval during which no more than one Hello packet can be sent. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. Increasing the hold-down timer limits the number of Hello packets triggered in response to Hello packets received from a neighboring node and reduces the likelihood of Hello packets flooding the OSC.

To configure the OSCP Hello hold-down timer, use the following global configuration command:

Command	Purpose
oscp timer hello holddown *milliseconds*	Configures the Hello hold-down timer in milliseconds. The default value is 3000 milliseconds.

Example

The following example shows how to set the Hello hold-down timer to 2000 milliseconds:

```
Switch(config)# oscp timer hello holddown 2000
```

Configuring the Inactivity Factor

The OSCP inactivity factor determines whether or not to declare a link down. The inactivity factor is multiplied by the advertised Hello timer interval of the other node to produce the inactivity time interval. If the system does not receive OSCP packets from the other node before the expiration of the inactivity time interval, the link is declared down.

To configure the OSCP inactivity factor, use the following global configuration command:

Command	Purpose
oscp timer inactivity-factor *factor*	Configures inactivity factor as a multiple of the Hello interval. The default multiplier is 5.

Example

The following example shows how to configure the inactivity factor to 10 times the Hello interval value:

```
Switch(config)# oscp timer inactivity-factor 10
```

Displaying the OSCP Configuration

You can display the OSCP version, node ID, interfaces, and configured protocol parameters. To display the OSCP configuration, use the following EXEC command:

Command	Purpose
show oscp info	Displays the OSCP configuration.

Example

The following example shows the OSCP configuration:

```
Switch(config)# show oscp info
OSCP protocol version 1, Node ID        0202.0304.0506
No. of interfaces 0, No. of neighbors 0
Hello interval 25 tenth of sec, inactivity factor 5,

Hello hold-down 1 tenth of sec
Supported OSCP versions: newest 1, oldest 1
```

Displaying OSCP Neighbors

You can display the information for neighboring nodes monitored by the OSCP. To display the OSCP neighbor status for a node, use the following EXEC command:

Command	Purpose
show oscp neighbor	Displays the OSCP neighbor status.

Example

The following example shows the OSCP neighbors for a node:

```
Switch(config)# show oscp neighbor
```

Configuring IP on the OSC

Configuring IP on the OSC allows you to use one Cisco ONS 15530 node in the network to monitor all the other Cisco ONS 15530 nodes in the network. The OSC is a point-to-point signal so any IP configuration valid for point-to-point interfaces is usable.

IP addressing on the OSC can be configured two ways:

- An IP address for each OSC wave interface with each address on a separate subnet.
- An unnumbered address for the OSC wave interfaces that reference another numbered interface.

  The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure IP address for each node in a separate subnet.

Note You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an OSC wave interface, perform the following steps, beginning in global configuration mode:

	Command	**Purpose**
Step 1	Switch(config)# **interface loopback 1** Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **ip address** *ip-address subnet-mask*	Configures IP address and subnet for the interface.
Step 3	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 4	Switch(config)# **interface fastethernet 0** Switch(config-if)#	Selects the NME interface to configuration and enters interface configuration mode.
Step 5	Switch(config-if)# **ip address** *ip-address subnet-mask*	Configures IP address and subnet for the interface.
Step 6	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 7	Switch(config)# **interface wave** *slot*/**0** Switch(config-if)#	Selects the wave interface in subcard 0.
Step 8	Switch(config-if)# **ip unnumbered loopback 1**	Configures an unnumbered interface referencing the loopback interface.
Step 9	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.

	Command	Purpose
Step 10	Switch(config)# **interface wave** *slot*/**1** Switch(config-if)#	Selects the wave interface in subcard 1.
Step 11	Switch(config-if)# **ip unnumbered loopback 1**	Configures an unnumbered interface referencing the loopback interface.
Step 12	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 13	Switch(config)# **ip route** *prefix prefix-mask interface* or Switch(config)# **router ospf** *process-id* Switch(config-router)# **network** *network-address wildcard-mask* **area** *area-id* or Switch(config)# **router eigrp** *as-number* Switch(config-router)# **network** *network-number* [*network-mask*] or Switch(config)# **router bgp** *as-number* Switch(config-router)# **network** *network-number* [**mask** *network-mask*] Switch(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	Configures IP static routes for some or all destinations. or Configures OSPF as the routing protocol. or Configures EIGRP as the routing protocol. or Configures BGP as the routing protocol.

Note For detailed information about configuring routing protocols, refer to the *Cisco IOS IP and IP Routing Configuration Guide*.

Example

The following example shows how to configure IP on the OSC on a three-node system. Node 1 connects to the NMS (network management system).

```
Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface wave 4/0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# ip unnumbered loopback 1
Node1(config)# router ospf 1
Node1(config-router)# network 10.1.0.0 0.0.255.255 area 0
Node1(config-router)# network 20.1.0.0 0.0.255.255 area 0
```

```
Node2# configure terminal
Node2(config)# interface loopback 1
Node2(config-if)# ip address 10.1.2.2 255.255.255.0
Node2(config-if)# exit
Node2(config)# interface wave 3/0
Node2(config-if)# ip unnumbered loopback 1
Node2(config-if)# exit
Node2(config)# interface wave 3/1
Node2(config-if)# ip unnumbered loopback 1
Node2(config)# router ospf 1
Node2(config-router)# network 10.1.0.0 0.0.255.255 area 0

Node3# configure terminal
Node3(config)# interface loopback 1
Node3(config-if)# ip address 10.1.3.3 255.255.255.0
Node3(config-if)# exit
Node3(config)# interface wave 2/0
Node3(config-if)# ip unnumbered loopback 1
Node3(config-if)# exit
Node3(config)# interface wave 2/1
Node3(config-if)# ip unnumbered loopback 1
Node3(config)# router ospf 1
Node3(config-router)# network 10.1.0.0 0.0.255.255 area 0
```

Displaying the OSC Configuration

To display the OSC configuration, use the following EXEC command:

Command	Purpose
show interfaces wave *slot*/*subcard*	Displays the OSC wave interface configuration.

Example

The following example shows the OSC configuration:

```
Switch# show interfaces wave 2/0
Wave2/0 is up, line protocol is up
  Channel: 0    Frequency: 191.9 Thz    Wavelength: 1562.23 nm
  Laser safety control: Off
  Osc physical port: Yes
  Wavelength used for inband management: No
  Configured threshold Group: None
  Last clearing of "show interface" counters never
  Hardware is OSC_phy_port
  Internet address is 1.0.0.3/16
  MTU 1492 bytes, BW 10000000 Kbit, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     13929 packets output, 919730 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Verifying Connectivity on the OSC

To verify connectivity over the OSC, use the following EXEC command:

Command	Purpose
telnet *ip-address*	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to use Telnet to connect from node 1 to node 2 in the ring to another node through the OSC:

```
Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#
```

Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel

Configuring IP on the in-band message channel allows you to use one Cisco ONS 15530 node in the network to monitor all the other Cisco ONS 15530 nodes in the network. The 10-Gbps ITU trunk cards and the 10-GE uplink cards support the in-band message channel.

IP addressing for the in-band message channel can be configured in two ways:

- An IP address for each ethernetdcc interface with each address on a separate subnet.
- An unnumbered address for the Ethernet interfaces that reference another numbered interface.

  The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure IP address for each node in a separate subnet. Refer also to "Interface Naming Conventions" section on page 2-4 for naming conventions.

Note You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an ethernetdcc interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface loopback 1** Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **ip address** *ip-address subnet-mask*	Configures IP address and subnet for the interface.
Step 3	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.

	Command	Purpose
Step 4	Switch(config)# **interface fastethernet 0** Switch(config-if)#	Selects the NME interface to configuration and enters interface configuration mode.
Step 5	Switch(config-if)# **ip address** *ip-address subnet-mask*	Configures IP address and subnet for the interface.
Step 6	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 7	Switch(config)# **interface ethernetdcc** *slot*/**0**/**0** Switch(config-if)#	Selects the ethernetdcc interface.
Step 8	Switch(config-if)# **ip unnumbered loopback 1**	Configures an unnumbered interface referencing the loopback interface.
Step 9	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 10	Switch(config)# **ip route** *prefix prefix-mask interface*	Configures IP static routes for some or all destinations.
	or	or
	Switch(config)# **router ospf** *process-id* Switch(config-router)# **network** *network-address wildcard-mask* **area** *area-id*	Configures OSPF as the routing protocol.
	or	or
	Switch(config)# **router eigrp** *as-number* Switch(config-router)# **network** *network-number* [*network-mask*]	Configures EIGRP as the routing protocol.
	or	or
	Switch(config)# **router bgp** *as-number* Switch(config-router)# **network** *network-number* [**mask** *network-mask*] Switch(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	Configures BGP as the routing protocol.

Note For detailed information about configuring routing protocols, refer to the *Cisco IOS IP and IP Routing Configuration Guide*.

Example

The following example shows how to configure IP on the OSC on a three node system. Node 1 connects to the NMS (network management system).

```
Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
```

```
Node1(config-if)# exit
Node1(config)# interface ethernetdcc 4/0/0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
```

Displaying the Ethernetdcc Interface Configuration

To display the ethernetdcc interface configuration, use the following EXEC command:

Command	Purpose
show interfaces ethernetdcc *slot*/*subcard*/*port*	Displays the IP ethernetdcc interface configuration.

Example

The following example shows how to display the IP configuration:

```
Switch# show interfaces ethernetdcc 4/0/0
EthernetDcc10/0/0 is up, line protocol is up
  Hardware is cdl_enabled_port
  Interface is unnumbered. Using address of Loopback1 (10.1.1.1)
  MTU 1492 bytes, BW 500000 Kbit, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     26156 packets input, 1569630 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     22 packets output, 2436 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Verifying Connectivity over the In-Band Message Channel

To verify connectivity over the in-band message channel, use the following EXEC command:

Command	Purpose
telnet *ip-address*	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to use Telnet to connect from node 1 to node 2 in the ring to another node through the in-band message channel:

```
Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#
```

Configuring SNMP

SNMP is an application-layer protocol that allows an SNMP manager, such an NMS (network management system), and an SNMP agent on the managed device to communicate. You can configure SNMPv1, SNMPv2c, or SNMPv3 on the Cisco ONS 15530.

The NME (network management Ethernet) ports on the active processor card, named *fastethernet 0*, provide multiple simultaneous SNMP network management sessions to the current active processor. The Cisco ONS 15530 can be fully managed by sending SNMP messages to the active processor IP address. If a processor switchover occurs, you can access the other processor card after it reaches the active state. For more information on processor card redundancy, see the "About CPU Switch Module Redundancy" section on page 3-8.

Note The standby processor card does not respond to SNMP messages.

For detailed instructions on configuring SNMP and enabling SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Enabling MIB Notifications

The Cisco ONS 15530 supports SMNP trap notifications through MIBs. This section describes the following MIBs:

- Alarm threshold MIB
- APS MIB
- CDL MIB
- Optical monitor MIB
- OSCP MIB
- Patch MIB
- Physical Topology MIB
- Redundancy facility MIB

You can find the complete list of MIBs supported on the Cisco ONS 15530 and the MIB definition files on the Cisco MIB website on Cisco.com. For more information on accessing the MIB definition files, refer to the *Cisco ONS 15530 MIB Quick Reference*.

Alarm Threshold MIB

The interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) assists SNMP monitoring of the interface alarm threshold activity. To enable the SNMP trap notifications for alarm threshold activity, use the following global configuration command:

Command	Purpose
snmp-server enable traps threshold min-severity {**degrade** | **failure**}	Enables SNMP trap notifications for alarm threshold activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for alarm thresholds and set the minimum notification severity to signal degrade.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps threshold min-severity degrade
```

APS MIB

The APS MIB (CISCO-APS-MIB) assists SNMP monitoring of SONET APS activity. To enable the SNMP trap notifications for APS activity between associated interfaces, use the following global configuration command:

Command	Purpose
snmp-server enable traps aps	Enables SNMP trap notifications for APS activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for APS.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps aps
```

CDL MIB

The CDL MIB (CISCO-CDL-MIB) assists SNMP monitoring of the in-band message channel activity. To enable the SNMP trap notifications for the in-band channel, use the following global configuration command:

Command	Purpose
snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *seconds*]	Enables SNMP trap notifications for the in-band message channel activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable all SNMP trap notifications for the in-band message channel activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Optical Monitor MIB

The APS MIB (CISCO-OPTICAL-MONITOR-MIB) assists SNMP monitoring of optical monitor activity. To enable the SNMP trap notifications for optical monitor, use the following global configuration command:

Command	Purpose
snmp-server enable traps optical monitor {critical | major | minor | not-alarmed}	Enables SNMP trap notifications for optical monitor activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable critical SNMP trap notifications for optical monitor activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps optical monitor critical
```

OSCP MIB

The OSCP MIB (CISCO-OSCP-MIB) assists SNMP monitoring of OSCP activity. To enable the SNMP trap notifications for OSCP activity, use the following global configuration command:

Command	Purpose
snmp-server enable traps oscp	Enables SNMP trap notifications for OSCP activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for OSCP.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps oscp
```

Patch MIB

The patch MIB (CISCO-OPTICAL-PATCH-MIB) assists SNMP monitoring of patch connections. To enable the SNMP trap notifications for patch connection creation, modification, and deletion, use the following global configuration command.

Command	Purpose
snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for patch connections:

```
Switch# configure terminal
Switch(config)# snmp-server enable traps patch
```

Physical Topology MIB

The network physical topology MIB (PTOPO-MIB) assists SNMP monitoring of network topology activity. To enable the SNMP trap notifications for network topology activity, use the following global configuration command.

Command	Purpose
snmp-server enable traps topology [**throttle-interval** *seconds*]	Enables SNMP trap notifications for network topology activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for network topology activity:

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

Redundancy Facility MIB

The redundancy facility MIB (CISCO-RF-MIB) assists SNMP monitoring of processor redundancy activity. To enable the SNMP trap notifications for processor redundancy activity, use the following global configuration command.

Command	Purpose
snmp-server enable traps rf	Enables SNMP trap notifications for the redundancy facility activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for processor redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Monitoring Without the OSC or In-Band Message Channel

To take advantage of the OSC, the Cisco ONS 15530 system must be equipped with oneOADM module with OSC (for unprotected configurations) or two OADM modules with OSC (for protected configurations). Likewise, to take advantage of the in-band message channel, the system must be equiped with a 10-Gbps ITU trunk card or a 10-GE uplink card. If your system is not equipped to support the OSC or in-band message channel, the following conditions apply:

- You cannot reach other nodes on the network using Telnet or SNMP. Separate connections to each system must exist on the network for management purposes.
- CDP does not function on the network. The physical topology must be configured manually for fault isolation and system management.
- Keepalive information is not available for other nodes on the network.

Setting up Connections to Individual Nodes

To access individual nodes in a Cisco ONS 15530 network without the OSC, you must establish separate connections to a management port on each system. This can be done using a Telnet session over an Ethernet connection, a console connection, or a modem connection to the auxiliary port. For instructions on how to do this, see Chapter 3, “Initial Configuration.”

For NMS without the OSC, each node reports individually to the NMS. Thus you must connect the NMS to each node using SNMP over an Ethernet connection.

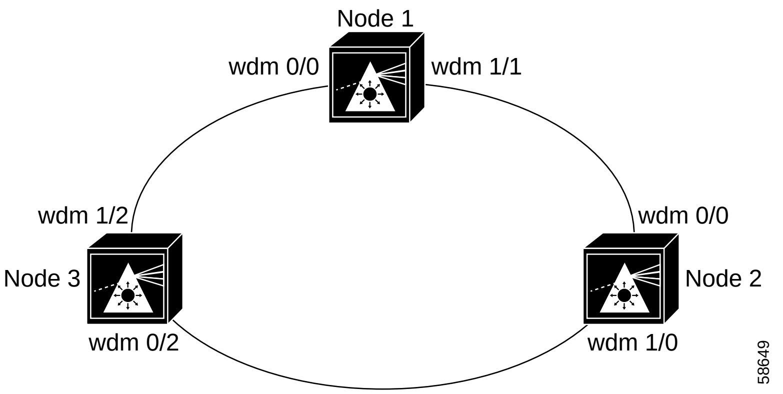
Manually Configuring the Network Topology

If the OSC is absent from the system or CDP is disabled, you must manually add the wdm interfaces connected to the trunk fiber to the network topology using the CLI. To manually add the wdm interfaces to the network topology, perform the following steps on all the nodes in the network, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface wdm** *slot/subcard* Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **topology neighbor** {**name** *node-name* | **ip-address** *node-ip-address* | **mac-address** *node-mac-address*} {**port** {**name** *port-name* | **ip-address** *port-ip-address* | **mac-address** *port-mac-address*}} [**receive** | **transmit**]	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# **topology neighbor agent ip-address** *ip-address*	Specifies the address of the network topology agent on a neighboring node.

Figure 9-2 shows an example ring topology with three shelves.

Figure 9-2 Ring Topology Example



The following example shows how to configure the network topology for node 1 in Figure 9-2:

```
Node1(config)# interface wdm 0/1
Node1(config-if)# topology neighbor name Node2 port name wdm0/0
Node1(config-if)# topology neighbor agent ip-address 10.2.2.2
Node1(config)# exit
Node1(config)# interface wdm 0/0
Node1(config-if)# topology neighbor name Node3 port name wdm0/1
Node1(config-if)# topology neighbor agent ip-address 10.3.3.3
```

The following example shows how to configure the network topology for node 2 in Figure 9-2:

```
Node2(config)# interface wdm 0/0
Node2(config-if)# topology neighbor name Node1 port name wdm0/1
Node2(config-if)# topology neighbor agent ip-address 10.1.1.1
Node2(config)# exit
Node2(config)# interface wdm 0/1
Node2(config-if)# topology neighbor name Node3 port name wdm0/0
Node2(config-if)# topology neighbor agent ip-address 10.3.3.3
```

The following example shows how to configure the network topology for node 3 in Figure 9-2:

```
Node3(config)# interface wdm 0/0
Node3(config-if)# topology neighbor name Node2 port name wdm0/1
Node3(config-if)# topology neighbor agent ip-address 10.2.2.2
Node3(config)# exit
Node3(config)# interface wdm 0/1
Node3(config-if)# topology neighbor name Node1 port name wdm0/0
Node3(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying the Network Topology

To display the network topology, use the following EXEC command:

Command	Purpose
show topology neighbor	Displays the network topology.

Example

The following example shows the network topology:

```
Switch# show topology neighbor

Physical Topology:

Local Port    Neighbor Node       Neighbor Port
----------    -------------       -------------
Wd0/0         Node1               wdm0/0
Wd0/1         Node2               wdm0/1
```

Configuring Interfaces in the Network Topology

Not all equipment connected to the Cisco ONS 15530 supports CDP topology discovery, such as client equipment connected to transparent or esconphy interfaces and EDFAs (erbium-doped fiber amplifiers) connected to wdm interfaces. To monitor this type of configuration, you must explicitly add these interfaces to the network topology.

To add a interfaces to the network topology, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface** {**transparent** *slot*/*subcard*/**0** | **wdm** *slot*/*subcard* | **esconphy** *slot*/*subcard*/*port* } Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **topology neighbor** {**name** *node-name* | **ip-address** *node-ip-address* | **mac-address** *node-mac-address*} {**port** {**name** *port-name* | **ip-address** *port-ip-address* | **mac-address** *port-mac-address*}} [**receive** | **transmit**]	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# **topology neighbor agent ip-address** *ip-address*	Specifies the address of the network topology agent on a neighboring node.

Example

The following example shows how to add a transparent interface to the network topology:

```
Switch(config)# interface transparent 8/0/0
Switch(config-if)# topology neighbor name router1 port name gigabitethernet1/1
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying Topology Information for Interfaces

To display the topology information for a transparent interface, use the following EXEC command:

Command	Purpose
show topology neighbor	Displays network topology information.

Example

The following example shows how to display the client equipment topology:

```
Switch# show topology neighbor

Physical Topology:

Local Port   Neighbor Node       Neighbor Port
----------   -------------       -------------
Trans8/0/0    Router1             gigabitethernet1/1
```

About Embedded CiscoView

The Embedded CiscoView network management system provides a web-based interface for the Cisco ONS 15530. Embedded CiscoView uses HTTP and SNMP to provide graphical representations of the system and to provide GUI-based management and configuration facilities. After you install and configure Embedded CiscoView, you can access your Cisco ONS 15530 from a web browser utility.

You can download the Embedded CiscoView files from the following URL:

http://www.cisco.com/kobayashi/sw-center/netmgmt/ciscoview/embed-cview-planner.shtml

Installing and Configuring Embedded CiscoView

To install and configure Embedded CiscoView on the Cisco ONS 15530, perform the following steps:

	Command	Purpose
Step 1	Switch# **copy tftp:** {**bootflash:** | **disk0:**}	Copies the CiscoView tar file (ONS15530.tar) from the TFTP server. If you are installing Embedded CiscoView for the first time, skip to Step 3.
Step 2	Switch# **delete** {**bootflash:** | **disk0:**}**cv/***	Removes existing files from the CiscoView directory.
Step 3	Switch# **archive tar /xtract disk0:ONS15530.tar** {**bootflash:** | **disk0:**}**cv**	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.
Step 4	Switch# **dir** {**bootflash:** | **disk0:**}	Displays the file in Flash memory. Repeat Step 1 and Step 4 for the file system on the standby processor (**sby-bootflash:** or **sby-disk0:**).
Step 5	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 6	Switch(config)# **ip http server**	Enables the HTTP web server.
Step 7	Switch(config)# **end** Switch#	Returns to privileged EXEC mode.
Step 8	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration in NVRAM.

Note Install Embedded CiscoView files only on disk0. Do not install the files on the bootflash.

Examples

The following example shows how to initially install Embedded CiscoView on both processors in your system:

```
Switch# copy tftp disk0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

Switch# archive tar /xtract disk0:ONS15530.tar disk0:/cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Switch# dir disk0:
Directory of disk0:/

    1  -rw-     2276396   Apr 30 2001 17:48:07  ONS15530-i-mz.121
    2  -rw-     1251840   May 23 2001 14:03:35  ONS15530.tar
    3  -rw-        8861   May 23 2001 14:26:05  cv/ONS15530-1.0.html
    4  -rw-     1183238   May 23 2001 14:26:06  cv/ONS15530-1.0.sgz
    5  -rw-        3704   May 23 2001 14:27:55  cv/ONS15530-1.0_ace.html
    6  -rw-         401   May 23 2001 14:27:55  cv/ONS15530-1.0_error.html
    7  -rw-       17003   May 23 2001 14:27:55  cv/ONS15530-1.0_jks.jar
    8  -rw-       17497   May 23 2001 14:27:57  cv/ONS15530-1.0_nos.jar
    9  -rw-        8861   May 23 2001 14:27:59  cv/applet.html
   10  -rw-         529   May 23 2001 14:28:00  cv/cisco.x509
   11  -rw-        2523   May 23 2001 14:28:00  cv/identitydb.obj

16384000 bytes total (1287752 bytes free)

Switch# copy tftp: sby-disk0:ONS15530.tar
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

Switch# archive tar /xtract disk0:ONS15530.tar sby-disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Switch# dir sby-disk0:
Directory of sby-disk0:/

    1  -rw-     2276396   May 20 2001 17:48:07  ONS15530-i-mz.121
    2  -rw-     1251840   May 23 2001 14:03:35  ONS15530.tar
    3  -rw-        8861   May 23 2001 14:26:05  cv/ONS15530-1.0.html
    4  -rw-     1183238   May 23 2001 14:26:06  cv/ONS15530-1.0.sgz
    5  -rw-        3704   May 23 2001 14:27:55  cv/ONS15530-1.0_ace.html
    6  -rw-         401   May 23 2001 14:27:55  cv/ONS15530-1.0_error.html
    7  -rw-       17003   May 23 2001 14:27:55  cv/ONS15530-1.0_jks.jar
    8  -rw-       17497   May 23 2001 14:27:57  cv/ONS15530-1.0_nos.jar
    9  -rw-        8861   May 23 2001 14:27:59  cv/applet.html
   10  -rw-         529   May 23 2001 14:28:00  cv/cisco.x509
   11  -rw-        2523   May 23 2001 14:28:00  cv/identitydb.obj
16384000 bytes total (1287752 bytes free)
```

```
Switch# configure terminal
Switch(config)# ip http server
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
```

The following example shows how to update the CiscoView files on your Cisco ONS 15530:

```
Switch# delete disk0:cv/*
Delete filename [cv/*]?
Delete disk0:cv/ONS15530-1.0.html? [confirm]
Delete disk0:cv/ONS15530-1.0.sgz? [confirm]
Delete disk0:cv/ONS15530-1.0_ace.html? [confirm]
Delete disk0:cv/ONS15530-1.0_error.html? [confirm]
Delete disk0:cv/ONS15530-1.0_jks.jar? [confirm]
Delete disk0:cv/ONS15530-1.0_nos.jar? [confirm]
Delete disk0:cv/applet.html? [confirm]
Delete disk0:cv/cisco.x509? [confirm]
Delete disk0:cv/identitydb.obj? [confirm]

Switch# copy tftp disk0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

Switch# archive tar /xtract disk0:ONS15530.tar disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Switch# delete sby-disk0:cv/*
Delete filename [cv/*]?
Delete disk0:cv/ONS15530-1.0.html? [confirm]
Delete disk0:cv/ONS15530-1.0.sgz? [confirm]
Delete disk0:cv/ONS15530-1.0_ace.html? [confirm]
Delete disk0:cv/ONS15530-1.0_error.html? [confirm]
Delete disk0:cv/ONS15530-1.0_jks.jar? [confirm]
Delete disk0:cv/ONS15530-1.0_nos.jar? [confirm]
Delete disk0:cv/applet.html? [confirm]
Delete disk0:cv/cisco.x509? [confirm]
Delete disk0:cv/identitydb.obj? [confirm]
Switch# copy tftp sby-disk0:
Address or name of remote host [20.1.1.1]?
Source filename [ONS15530.tar]?
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)
Switch# archive tar /xtract disk0:ONS15530.tar disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Switch# archive tar /xtract tftp://10.1.1.1/ciscoview.tar sby-disk0:cv
```

Accessing Embedded CiscoView

Access Embedded CiscoView using the NME IP address as the URL for your Cisco ONS 15530 from a web browser using the following format:

http://*A.B.C.D*/

Displaying Embedded CiscoView Information

To display the Embedded CiscoView information, use the following EXEC commands:

Command	Purpose
show ciscoview package	Displays information about the Embedded CiscoView files in the Flash PC Card.
show ciscoview version	Displays the Embedded CiscoView version.

Example

The following example shows how to display the Embedded CiscoView file and version information:

```
Switch# show ciscoview package
File source:disk0:
CVFILE                          SIZE(in bytes)
------------------------------------------------
ONS15530-1.0.html                8861
ONS15530-1.0.sgz                 1183238
ONS15530-1.0_ace.html            3704
ONS15530-1.0_error.html          401
ONS15530-1.0_jks.jar             17003
ONS15530-1.0_nos.jar             17497
applet.html                      8861
cisco.x509                       529
identitydb.obj                   2523

Switch# show ciscoview version
Engine Version: 5.3 ADP Device: ONS15530 ADP Version: 1.0 ADK: 39
```

CHAPTER 10

Managing Your Cisco ONS 15530 System

This chapter describes how to manage system images, functional images, and configuration files. This chapter includes the following sections:

- Accessing and Displaying File System Devices, page 10-1
- Using Flash Memory, page 10-2
- Accessing System Images on TFTP Servers, page 10-6
- Updating System Images, page 10-11
- Updating Functional Images, page 10-19

Accessing and Displaying File System Devices

The active processor can read, write, and format files on both the active and standby CPU switch modules. To access devices on the standby CPU switch module from the active CPU switch module, add the prefix “sby-” to the device name.

To display the contents of a file system directory and copy files, use the following commands at the active processor CLI (command-line interface):

Command	Purpose
dir [*fs-name*]	Displays the contents of a file system directory.
copy *fs-name1*[*filename1*] *fs-name2*[*filename2*]	Copies files from one file system to another.

Examples

The following example shows the file system devices accessible from the active CPU switch module:

```
Switch# dir ?
  /all             List all files
  /recursive       List files recursively
  all-filesystems  List files on all filesystems
  bootflash:       Directory or file name
  disk0:           Directory or file name
  null:            Directory or file name
  nvram:           Directory or file name
  sby-bootflash:   Directory or file name
  sby-disk0:       Directory or file name
  sby-nvram:       Directory or file name
  system:          Directory or file name
  <cr>
```

The following example shows how to copy a file from the CompactFlash card on the active CPU switch module to the bootflash: on the active CPU switch module:

```
Switch# copy disk0:ons15530-i-mz.1 bootflash:ons15530-i-mx.1
```

The following example shows the contents of the standby CPU switch module bootflash directory listed on a terminal accessing the active CPU switch module:

```
Switch# dir sby-bootflash:
Directory of sby-bootflash:/

    1  -rw-         772   May 29 2001 11:28:51  running-
    2  -rw-     2452192   May 29 2001 11:27:34 ons15530-i-mz.1
```

Using Flash Memory

This section describes how to use onboard Flash memory, or bootflash memory, and CompactFlash cards to copy system images and make standard configurations. CompactFlash cards use a type of Flash memory that provide expanded file storage for your Cisco ONS 15530. CompactFlash cards, unlike the onboard Flash memory SIMM (bootflash), are not required for the operation of the system.

CompactFlash cards store a copy of the system image. The following sections describe how to format, delete, configure, and copy files between the onboard Flash memory SIMM (Single In-Line Memory Module), network servers, and CompactFlash cards.

Formatting CompactFlash Cards

A newly purchased CompactFlash card is blank and must be formatted before use.

Caution The formatting procedure erases all information on the CompactFlash card.

After inserting the CompactFlash card, format it using the following privileged EXEC command:

Command	Purpose
format disk0:	Formats the CompactFlash card.

Example

The following example shows how to format a CompactFlash card:

```
Switch# format disk0:

Format operation may take a while. Continue? [confirm] y
Format operation will destroy all data in `disk0:'.  Continue? [confirm] y
Format:Drive communication & 1st Sector Write OK...
Writing Monlib
sectors.....................................................................
.......................
Monlib write complete

Format:All system sectors written. OK...

Format:Total sectors in formatted partition:81760
Format:Total bytes in formatted partition:49861120
Format:Operation completed successfully.

Format of disk0:complete
```

Note For more information on inserting a CompactFlash card, refer to the *Cisco ONS 15530 Hardware Installation Guide*.

Copying the Startup Configuration Files to Flash Memory

To copy the startup configuration file from NVRAM to bootflash memory or to a CompactFlash card, once the CompactFlash card is formatted and ready to use, use the following privileged EXEC command:

Command	Purpose
copy nvram:startup-config {**bootflash:** | **disk0:** | **sby-disk0:**}	Copies the startup-config file from NVRAM to Flash memory.

Example

The following example shows how to copy the startup configuration file to the CompactFlash card; the default filename is used:

```
Switch# copy nvram:startup-config disk0:
Destination filename [startup-config]? y
386 bytes copied in 0.268 secs
Switch#
```

Copying Files Between Flash Memory Devices

On platforms with multiple Flash memory file systems, you can copy files from one Flash memory file system, such as internal Flash memory or a CompactFlash card, to another Flash memory file system. Copying files to different Flash memory file systems lets you create backup copies of working configurations, duplicate configurations for other devices, and make copies of system images.

The following example describes how to copy a new system image from Flash memory on the active CPU switch module to a Flash memory on the standby CPU switch module that contains an old system image. If you are copying to a CompactFlash card, first insert the CompactFlash card in the target CPU switch module.

Tips Make sure that the new system image file fits on the CompactFlash card in the standby CPU switch module along with the old system image file.

To copy the new system image file from the CompactFlash card on the active CPU switch module to the CompactFlash card on the standby CPU switch module that contains the old system image file, enter this command from privileged EXEC mode:

```
Switch# copy disk0:image.new sby-disk0:image.new
```

Viewing the Contents of Flash Memory

This section describes commands you can use with the onboard Flash memory SIMM (bootflash) and CompactFlash cards.

Determining the Current File System Device

To determine which file system device you are accessing, use the **pwd** (print working directory) command, as shown in the following example:

```
Switch# pwd
disk0:/
```

Moving Between Flash Memory Devices

To move between Flash memory devices, use the **cd** command, as shown in the following example:

```
Switch# cd bootflash:
Switch# pwd
bootflash:/
```

Listing the Flash Memory Directory Contents

To list the directory contents of any Flash memory media, use the **dir** command, as shown in the following example:

```
Switch# dir disk0:
Directory of disk0:/

    1 -rw-     2438216   May 21 2001 11:44:35  ons15530-i-mz.1
    2 -rw-     2426828   May 23 2001 16:02:49  ons15530-i-mz.2
```

Deleting Files from Bootflash Memory

When you delete a file from bootflash memory, the system marks the file as deleted, allowing you to later recover a deleted file using the **undelete** command. Erased files cannot be recovered. To permanently erase the configuration file, use the **squeeze** command.

The **squeeze** command permanently removes files marked for deletion, and pushes all the other undeleted files together to eliminate spaces between them. To prevent data loss due to sudden power loss, the "squeezed" data is temporarily saved to another location in bootflash memory. The **squeeze** command keeps a log of the functions performed so that if a power failure occurs, the system continues the process when the power resumes.

Caution When deleting files from memory, be careful not to delete all the system images. If you delete all existing system images, you can no longer boot the system from local memory.

For an example of using the **delete** and **squeeze** commands, see the "Updating with Hot-Standby Compatible System Images" section on page 10-15.

Copying a System Image from a TFTP Server to Flash Memory

You can copy system image files from a TFTP server to Flash memory for use in booting the Cisco ONS 15530 or for backup purposes. If the system image on internal Flash memory becomes corrupted, you can replace the system software by copying the backup system image from the CompactFlash card to the onboard Flash memory.

To create a backup of the system software on a TFTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **show** {**bootflash:** | **disk0:** | **sby-disk0:**}	Displays the contents of the specified Flash memory device, including the amount of free space that is available. If enough free space is available, skip to Step 4
Step 2	Switch# **delete** {**bootflash:** | **disk0:** | **sby-disk0:**} *filename*	Deletes an old file to make room for the new file.
Step 3	Switch# **squeeze bootflash:**	Recovers the space used by the files marked as deleted on onboard Flash memory. This command is not necessary for CompactFlash cards.
Step 4	Switch# **copy tftp:** {**bootflash:** | **disk0:** | **sby-disk0:**}	Copies a file from a TFTP server to a Flash memory device.

Example

The following example shows how to copy a system image file from the default TFTP server to the CompactFlash card:

```
Switch# copy tftp: disk0:
Address or name of remote host []? 172.68.16.129
Source filename []? ons15530-i-mz
Destination filename [ons15530-i-mz]? y
```

Booting from a CompactFlash Card

The Cisco ONS 15530 can be booted, automatically or manually, from a variety of sources, including a network server or Flash memory device. This section describes how to configure the Cisco ONS 15530 to boot automatically from an system image on a CompactFlash card. For an example of configuring the system to boot manually from a CompactFlash card, see the "Updating System Images" section on page 10-11.

To enable booting from a CompactFlash card, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# **no boot system**	Disables booting from bootflash.
Step 3	Switch(config)# **boot system flash** [**bootflash:** | **disk0:**][*partition-number***:**][*filename*]	Enables booting from the specified system image on the specified Flash file system.
Step 4	Switch(config)# **config-register 0x2102**	Sets the configuration register for automatic booting.[1]
Step 5	Switch(config)# **end** Switch#	Exits global configuration mode.
Step 6	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration to NVRAM.
Step 7	Switch# **reload**	Reboots the system.

[1] This is the default configuration register setting. For details on using the configuration register to set boot parameters, refer to the "Initial Configuration" chapter.

When you enter **boot system** commands, be careful not to insert extra spaces because they influence the way the system interprets the command. Notice the difference in the following examples:

Examples

The following command correctly instructs the system to boot the *image1* file in onboard Flash memory.

```
Switch(config)# boot system flash bootflash:image1
```

The following command incorrectly contains a space between "disk0:" and "image2." The system finds the *filename* field blank and so boots the first file on the CompactFlash card.

```
Switch(config)# boot system flash disk0: image2
```

Accessing System Images on TFTP Servers

For ease of management, the Cisco ONS 15530 can access TFTP servers for booting and archiving purposes. This sections describes how to access system images on a TFTP server.

Booting from a TFTP Server

This section describes how to configure the Cisco ONS 15530 to boot a system image located on a TFTP server. To boot the standby CPU switch module with an image located on a TFTP server, you must configure the fastethernet-sby 0 interface with a unique IP address on a subnet separate from the subnet used by the fastethernet 0 interface. This configuration prevents conflicts with the fastethernet 0 interface on the active CPU switch module.

Note The IP address and subnet mask must be different from the IP address and subnet mask for the fastethernet 0 interface on the active processor

To configure booting of a system image located on a TFTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# **config-register 0x2102** or Switch(config)# **config-register 0x0**	Sets the configuration register for automatic booting.[1] Sets the configuration register for manual booting.
Step 3	Switch(config)# **boot system tftp:***filename* [*ip-address*]	Enables booting a system image located on a TFTP server for automatic booting.
Step 4	Switch(config)# **interface fastethernet 0** Switch(config-if)#	Enters interface configuration mode for interface fastethernet 0, the NME interface on the active CPU switch module.
Step 5	Switch(config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and IP subnet mask for the active NME interface.
Step 6	Switch(config-if)# **speed** {**10** | **100** | **auto**}	Specifies the transmission speed. The default is **auto** (autonegotiation).
Step 7	Switch(config-if)# **duplex** {**auto** | **full** | **half**}	Specifies the duplex mode. The default is **auto** (autonegotiation).
Step 8	Switch(config-if)# **exit** Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 9	Switch(config)# **interface fastethernet-sby 0** Switch(config-if)#	Enters interface configuration mode for interface fastethernet-sby 0, the NME interface on the standby CPU switch module.
Step 10	Switch(config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and IP subnet mask for the standby NME interface. **Note** The IP address and subnet mask must be different from the IP address and subnet mask for the NME interface on the active processor.

	Command	Purpose
Step 11	Switch(config-if)# **speed** {**10** | **100** | **auto**}	Specifies the transmission speed. The default is **auto** (autonegotiation). **Note** The speed must be the same as the speed configured on the NME interface on the active CPU switch module for processor switchovers to succeed.
Step 12	Switch(config-if)# **duplex** {**auto** | **full** | **half**}	Specifies the duplex mode. The default is **auto** (autonegotiation). **Note** The duplex mode must be the same as the duplex mode configured on the NME interface on the active CPU switch module for processor switchovers to succeed.
Step 13	Switch(config-if)# **end** Switch#	Exits interface configuration mode.
Step 14	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration to NVRAM.
Step 15	Switch# **reload**	Reboots the system.

[1] This is the default configuration register setting. For details on using the configuration register to set boot parameters, refer to the "Initial Configuration" chapter.

Note You cannot use the IP address on the fastethernet-sby 0 interface for Telnet sessions or for network management system sessions.

For more information on booting system images, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

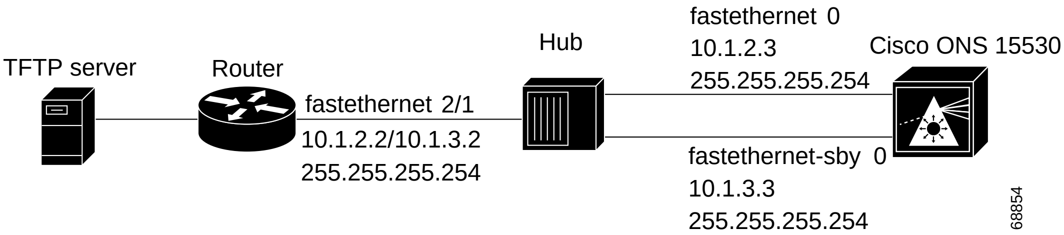
Examples

The following example shows how to configure the Cisco ONS 15530 to automatically boot using a system image located on a TFTP server.

```
Switch> enable
Switch# configure terminal
Switch(config)# boot system tftp ons15530-i-mz.1 172.20.51.30
Switch(config)# config-register 0x2102
Switch(config)# interface fastethernet 0
Switch(config-if)# ip address 172.20.42.105 255.255.255.254
Switch(config-if)# speed 100
Switch(config-if)# duplex full
Switch(config-if)# exit
Switch(config)# interface fastethernet-sby 0
Switch(config-if)# ip address 172.20.42.106 255.255.255.254
Switch(config-if)# speed 100
Switch(config-if)# duplex full
Switch(config-if)# end
Switch# copy system:running-config nvram:startup-config
Switch# reboot
```

Figure 10-1 shows a simple network configuration with a TFTP server, a router, a hub, and a Cisco ONS 15530.

Figure 10-1 Example Network with TFTP Server, Router, Hub, and Cisco ONS 15530

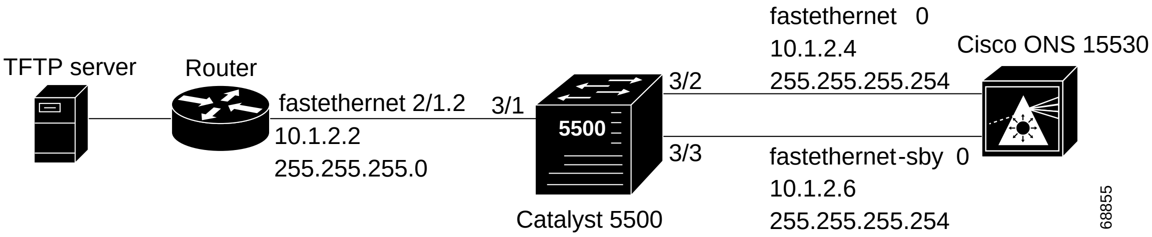


The following example shows how to configure the network example shown in Figure 10-1.

```
router(config)# interface fastethernet2/1
router(config-if)# ip address 10.1.2.2 255.255.255.254
router(config-if)# ip address 10.1.3.2 255.255.255.254 secondary

ons15530(config)# interface fastethernet 0
ons15530(config-if)# ip address 10.1.2.3 255.255.255.254
ons15530(config-if)# exit
ons15530(config)# interface fastethernet-sby 0
ons15530(config-if)# ip address 10.1.3.3 255.255.255.254
```

Figure 10-2 shows a simple network configuration with a TFTP server, a router, a Catalyst 5500, and a Cisco ONS 15530.

Figure 10-2 Example Network with TFTP Server, Router, Catalyst 5500, Cisco ONS 15530, and VLAN Trunk

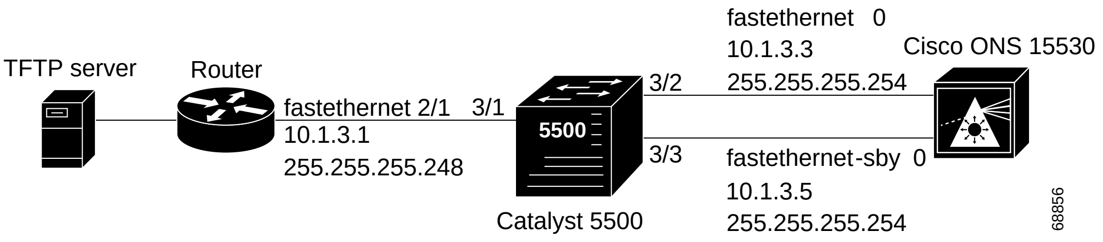


The following example shows how to configure the network example shown in Figure 10-2 with a VLAN trunk.

```
router(config)# interface fastethernet2/1.2
router(config-subif)# encapsulation isl 2
router(config-subif)# ip address 10.1.2.2 255.255.255.0

Cat5500> (enable) set vtp domain Corporate
Cat5500> (enable) set vtp mode server
Cat5500> (enable) set vlan 2
Cat5500> (enable) set vlan 2 3/2
Cat5500> (enable) set vlan 2 3/3
Cat5500> (enable) set trunk 3/1 on

ons15530(config)# interface fastethernet 0
ons15530(config-if)# ip address 10.1.2.4 255.255.255.254
ons15530(config-if)# exit
ons15530(config)# interface fastethernet-sby 0
ons15530(config-if)# ip address 10.1.2.6 255.255.255.254
```

Figure 10-3 shows a simple network configuration with a TFTP server, a router, a Catalyst 5500, and a Cisco ONS 15530.

Figure 10-3 Example Network with TFTP Server, Router, Catalyst 5500, Cisco ONS 15530, and VLAN



The following example shows how to configure the network example shown in Figure 10-3 with a VLAN.

```
router(config)# interface fastethernet2/1
router(config-if)# ip address 10.1.3.1 255.255.255.248

Cat5500> (enable) set vlan 2
Cat5500> (enable) set vlan 2 3/1
Cat5500> (enable) set vlan 2 3/2
Cat5500> (enable) set vlan 2 3/3

ons15530(config)# interface fastethernet 0
ons15530(config-if)# ip address 10.1.3.3 255.255.255.254
ons15530(config-if)# exit
ons15530(config)# interface fastethernet-sby 0
ons15530(config-if)# ip address 10.1.3.5 255.255.255.254
```

Backing Up a System Image to a TFTP Server

To create a backup copy of your system image, or to verify that the copy in Flash memory is the same as the original file on disk, you can copy system images from Flash memory to a TFTP (Trivial File Transfer Protocol) server.

In some implementations of TFTP, you must create a dummy file on the TFTP server and give it read, write, and execute permissions before copying the file over it. Refer to your TFTP documentation for more information.

Before you copy software between the network server and Flash memory in the router, do the following:

- Make sure you have access to the network server, and obtain its IP address and name.
- Verify that the server has sufficient room to accommodate the Cisco IOS system image.
- Check the filename requirements and file space of the network server.
- Create a dummy file on the server with read-write-execute permission. You copy the system image to this file.

To create a backup of the system software on a TFTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **show** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**}	Displays the contents of the specified Flash memory device, including the names of the system images that currently reside there. Note the name of the system image file you want to copy.
Step 2	Switch# **copy** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**} **tftp:**	Copies a file from a Flash memory device to a TFTP server.

Example

The following example shows how to copy a specified system image file from the current Flash memory device to the default TFTP server:

```
Switch# copy disk0: tftp:
Address or name of remote host []? 172.68.16.129
Source filename [] ons15530-i-mz
Destination filename [ons15530-i-mz]? y
```

Updating System Images

This section provides minimal instructions for updating system images on your Cisco ONS 15530. The default system configuration causes the system to boot automatically from the system image specified in the BOOT environment variable. This procedure also describes now to update and manually boot the system from a system image on a CompactFlash card. For additional information on booting options and maintaining system images, refer to the Cisco IOS Configuration Fundamentals Configuration Guide.

Downloading System Images from Cisco.com

Cisco IOS system images, along with other software, are available from the Software Center on Cisco.com at http://www.cisco.com. You can download system images from Cisco.com using your browser’s FTP capability, using conventional FTP, or using Cisco.com asynchronous dial-up interface.

For instructions on accessing and downloading software from Cisco.com, refer to the document “Using the Software Center” at the Software Center on Cisco.com.

Copying System Images to the Cisco ONS 15530

You can copy the system image to the Cisco ONS 15530 using either TFTP, FTP, or RCP. If the system you used to download the system image from Cisco.com does not function as a TFTP, FTP, or RCP server, you must first copy the file to an intermediate server that provides those services to your system.

Note Before copying the system image from the server to the system, check the size of the file to make sure you have enough room for it on the Flash memory device. On UNIX file systems, use the **ls -la** command from the directory where the file is stored to display the file size.

Note Be sure that you have a properly formatted the CompactFlash card before beginning this procedure.

To copy the system image from a TFTP server to the Flash memory, initiate a Telnet session or console connection to the system and perform the following steps in privileged EXEC mode:

	Command	Purpose
Step 1	Switch# **dir** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**}	Displays the contents and available space on the Flash memory device. If there is not enough free space to copy the new system image, perform Step 2 and Step 4. Otherwise, proceed to Step 5.
Step 2	Switch# **delete** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**}*filename*	Marks a file as deleted. If you have older system images stored on the file system, we recommend that you delete the oldest one and leave a newer one in case you need to revert.
Step 3	Switch# **squeeze** {**bootflash:** | **sby-bootflash:**}	Recovers the space used by the files marked as deleted on onboard Flash memory. This command is not necessary for CompactFlash cards.
Step 4	Switch# **copy tftp:** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**}	Initiates a TFTP session to copy the system image from the TFTP server. The system prompts you for a TFTP server name and filename.
Step 5	Switch# **dir** {**bootflash:** | **disk0:** | **sby-disk0:** | **sby-bootflash:**}	Displays the contents of the file system. This step confirms that the file was copied as expected.

Example

The following example shows how to delete a file from the CompactFlash card and copy a new system image to it using TFTP:

```
Switch# dir disk0:
Directory of disk0:/
    1 -rw-     2538248    Dec 05 2001 01:42:30  ons15530-i-mz.121-7a.EY2.bin

20578304 bytes total (18040056 bytes free)
Switch# delete disk0:ons15530-i-mz.121-7a.EY2.bin
Delete filename [ons15530-i-mz.121-7a.EY2.bin]? y
Delete disk0:ons15530-i-mz.121-7a.EY2 [confirm] y
```

```
Switch# copy tftp: disk0:
Address or name of remote host [] mocha
Source filename [] joe/ons15530-i-mz
Destination filename [ons15530-i-mz]
Switch# dir disk0:
Directory of disk0:/


20530200 bytes total (20530200 bytes free)
```

Note Be sure that the file size is the same after it was copied as it is on the server.

Manually Booting the Cisco ONS 15530

When the configuration register is set for manual booting, issuing the **reload** command causes the system to enter ROM monitor mode, where you enter the **boot** command and the name of the system image to use. To perform this procedure, you must be connected to the console port, which provides access to a system in ROM monitor mode. For automatic booting you can issue the **reload** command from an Ethernet connection to the processor.

Note This procedure assumes that you need to change the boot field in the configuration register from its default value so that the system reverts to ROM monitor mode when the **reload** command is issued.

To reload the Cisco ONS 15530 with the new system image on the CompactFlash card, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **config-register 0x0**	Sets the configuration register for manual booting from ROM monitor mode.[1]
Step 2	Switch(config)# **end** Switch#	Returns to privileged EXEC mode.
Step 3	Switch# **copy system:running-config nvram:startup-config**	Saves your configuration changes to NVRAM.
Step 4	Switch# **reload**	Initiates a reload of the system software. The system prompts you to save the modified configuration before you can proceed. You then enter ROM monitor mode.
Step 5	rommon 1> **dir** *filesystem***:**	Displays the contents of the file system. Perform this optional step to display and copy the name of the system image to the clipboard for use in the next step.
Step 6	rommon 2> **boot** *filesystem***:***filename*	Reboots the system with the new system image. You can paste the filename from the clipboard if you copied it in the previous step.
Step 7	Switch> **show version**	Displays the system software version information. Use this step to confirm that the system is loaded with the expected software version.

[1] For details on using the configuration register to set boot parameters, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Example

The following example shows how to set the configuration register, save the configuration, and reload the Cisco ONS 15530 with the new system image on the CompactFlash card:

```
Switch(config)# config-register 0x0
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch# reload
System configuration has been modified. Save? [yes/no]: y
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm] y
Building configuration...
[OK]
Proceed with reload? [confirm]
rommon 1> dir disk0:
Directory of disk0:/
    1  -rw-     2506076   Jan 01 2000 00:59:36  ons15530-i-mz.121-99.UBLDIT188
    2  -rw-     2519840   Jan 01 2000 00:02:01  ons15530-i-mz.121-99.UBLDT020101

20530200 bytes total (6270284 bytes free)
rommon 2> boot disk0:ons15530-i-mz.121-99.UBLDIT188

<The system boots.>

Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) ONS-15530 Software (ONS15530-I-M)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 15-Aug-01 13:32 by jko
Image text-base: 0x60010950, data-base: 0x60630000

ROM: System Bootstrap, Version 12.1(20010726:234219) [ffrazer-lh4 102], DEVELOPMENT
SOFTWARE

man1 uptime is 14 hours, 59 minutes
System returned to ROM by reload
System image file is "disk0:ons15530-i-mz"

cisco ONS15530 (QUEENS-CPU) processor with 98304K/32768K bytes of memory.
R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

Last reset from power-on
2 FastEthernet/IEEE 802.3 interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
```

Updating System Images on Redundant Processors

The Cisco ONS 15530 supports software upgrades and downgrades with no interruption of data traffic. You can enter all commands from the currently active processor console connection or Telnet session.

The following upgrade procedures allow you to qualify a new image on one CPU switch module while optionally keeping an older trusted image on the redundant peer CPU switch module.

Caution If you are upgrading or downgrading with system images that differ by more than one major release, the standby CPU switch module might not reach the hot-standby state. If a switchover occurs while not in the hot-standby state, there is a risk of loss of the configuration. If the processor cannot reach the hot-standby state, use the procedure described in the "Updating with Non-Hot-Standby Compatible System Images" section on page 10-17.

Updating with Hot-Standby Compatible System Images

The following procedure describes how to copy a new hot-standby compatible system image from the network to the bootflash device.

Step 1 Verify that the system is configured with the default auto-boot configuration, automatic synchronization enabled for both the running-config and startup-config files, and the standby processor in the hot-standby software state.

Step 2 Copy the new system image to the standby CPU switch module bootflash using the CLI on the active CPU switch module. Delete the old system image from the standby processor bootflash if there is not room.

Note Make sure the active CPU switch module bootflash only contains the old system image name and not the new system image name.

Step 3 Rearrange any existing **boot system** commands so the new system image appears as the first boot image on the list. Optionally, you can configure the original system image as the second boot image.

Note Because the new system image is only present on the standby CPU switch module bootflash, only the standby CPU switch module will load it. When the former active CPU switch module reloads, it will load the original system image after trying and failing to load the missing new system image.

Step 4 Reload the original standby processor with the new system image and make sure it goes to the hot-standby state. (At this point, we recommend that you copy the running-config file to the startup-config file before continuing.)

Step 5 Initiate a switchover that causes the new system image reload on the new active CPU switch module. After the switchover, verify that the new standby CPU switch module, which is running the original system image, goes to the hot-standby state.

Step 6 Configure new features, and, if desired, qualify the new system image for an extended period of time on the new active CPU switch module with the old system image running on the standby CPU switch module.

Note If a switchover occurs back to a processor running an older system image, all configuration commands supported by the older software version are retained. Any new configuration features do not appear in the running configuration. New configuration features saved in the startup configuration will remain.

Step 7 Copy the new system image to the other processor after qualifying the new system image, and, if desired, delete the old system image.

Step 8 Reload the new system image on the standby CPU switch module.

To update the system images on redundant processors, perform the following steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Switch> **enable**	Enters privileged EXEC mode on the active CPU switch module NME interface.
Step 2	Switch# **show version**	Displays the configuration register contents. The default autoconfiguration value is 0x2102.
Step 3	Switch# **show bootvar**	Displays the automatic database synchronization configuration.
Step 4	Switch# **show redundancy**	Displays the hardware and software redundancy states of the CPU switch modules.
Step 5	Switch# **dir sby-bootflash:**	Displays the contents and available space on the Flash memory device on the standby processor. If there is not enough free space to copy the new system image, perform Step 6 and Step 7. Otherwise, proceed to Step 8.
Step 6	Switch# **delete sby-bootflash:***filename*	Marks a file as deleted on the standby CPU switch module. If you have older system images stored on the file system, we recommend that you delete the oldest one and leave a newer one in case you need to revert.
Step 7	Switch# **squeeze sby-bootflash:**	Recovers the space used by the files marked as deleted.
Step 8	Switch# **copy tftp:***new-image-name* **sby-bootflash:**	Initiates a TFTP session to copy the system image from the TFTP server to the Flash memory device on the standby CPU switch module. The system prompts you for a TFTP server name and filename.
Step 9	Switch# **dir sby-bootflash:**	Displays the contents of the standby CPU switch module file system and confirms that the file was copied as expected.
Step 10	Switch# **configure terminal**	Enters global configuration mode.
Step 11	Switch(config)# **boot system bootflash:***new-image-name*	Adds the new system image to the system boot list.
Step 12	Switch(config)# **no boot system bootflash:***old-image-name*	Removes the old system image from the top of the system boot list.
Step 13	Switch(config)# **boot system bootflash:***old-image-name*	Adds the old system image to the system boot list after the new system image.
Step 14	Switch(config)# **exit**	Exits global configuration mode.
Step 15	Switch# **show running-config**	Shows the current running configuration to verify the order of the **boot system** commands. The new system image should appear first.
Step 16	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration to NVRAM.

	Command	Purpose
Step 17	Switch# **copy system:running-config tftp:**	Saves the configuration to a TFTP server. (Optional)
Step 18	Switch# **redundancy reload peer**	Initiates a reload of the system image on the standby CPU switch module.
Step 19	Switch# **show redundancy**	Displays the CPU switch module redundancy status and images Verify that the standby CPU switch module is running the desired new image. **Note** If the standby CPU switch module fails to reach the hot-standby state, follow the procedure described in the "Updating with Non-Hot-Standby Compatible System Images" section on page 10-17.
Step 20	Switch# **redundancy switch-activity**	Switches system control over to the standby CPU switch module by reloading the system image on the active CPU switch module. Repeat Step 1 through Step 9 and then Step 16 through Step 19 if no problems occur with the new system image on the active CPU switch module.

Updating with Non-Hot-Standby Compatible System Images

System images with widely different version numbers might not allow the standby CPU switch module to reach hot-standby state. A different upgrade procedure is necessary to handle these cases.

Caution This procedure might cause a short data interruption, unlike the procedure described in the previous section, "Updating with Hot-Standby Compatible System Images."

To update between system images that are not hot-standby compatible, perform the following steps on the active CPU switch module:

	Command	Purpose
Step 1	Switch> **enable** Switch#	Enters privileged EXEC mode on the active CPU switch module NME interface.
Step 2	Switch# **show version**	Displays the configuration register contents. The default autoconfiguration value is 0x2102.
Step 3	Switch# **show bootvar**	Displays the automatic database synchronization configuration.
Step 4	Switch# **show redundancy**	Displays the hardware and software redundancy states of the CPU switch modules.
Step 5	Switch# **dir bootflash:**	Displays the contents and available space on the Flash memory device on the active CPU switch module. If there is not enough free space to copy the new system image, perform Step 6 and Step 7. Otherwise, proceed to Step 8.

	Command	Purpose
Step 6	Switch# **delete bootflash:***filename*	Marks a file as deleted on the active CPU switch module. If you have older system images stored on the file system, we recommend that you delete the oldest one and leave a newer one in case you need to revert.
Step 7	Switch# **squeeze bootflash:**	Recovers the space used by the files marked as deleted.
Step 8	Switch# **copy tftp:***new-image-name* **bootflash:**	Initiates a TFTP session to copy the system image from the TFTP server to the Flash memory device on the active CPU switch module. The system prompts you for a TFTP server name and filename.
Step 9	Switch# **dir bootflash:**	Displays the contents of the active CPU switch module file system and confirms that the file was copied as expected.
Step 10	Switch# **dir sby-bootflash:**	Displays the contents and available space on the Flash memory device on the standby CPU switch module. If there is not enough free space to copy the new system image, perform Step 11 and Step 12. Otherwise, proceed to Step 13.
Step 11	Switch# **delete sby-bootflash:***filename*	Marks a file as deleted on the standby CPU switch module. If you have older system images stored on the file system, we recommend that you delete the oldest one and leave a newer one in case you need to revert.
Step 12	Switch# **squeeze sby-bootflash:**	Recovers the space used by the files marked as deleted.
Step 13	Switch# **copy tftp:***new-image-name* **sby-bootflash:**	Initiates a TFTP session to copy the system image from the TFTP server to the Flash memory device on the standby CPU switch module. The system prompts you for a TFTP server name and filename.
Step 14	Switch# **dir sby-bootflash:**	Displays the contents of the standby CPU switch module file system and confirms that the file was copied as expected.
Step 15	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 16	Switch(config)# **boot system bootflash:***new-image-name*	Adds the new system image to the system boot list.
Step 17	Switch(config)# **no boot system bootflash:***old-image-name*	Removes the old system image from top of the system boot list.
Step 18	Switch(config)# **boot system bootflash:***old-image-name*	Adds the old system image to the system boot list after the new system image.
Step 19	Switch(config)# **exit** Switch#	Exits global configuration mode.
Step 20	Switch# **show running-config**	Shows the current running configuration to verify the order of the **boot system** commands. The new system image should appear first.
Step 21	Switch# **copy system:running-config nvram:startup-config**	Saves the configuration to NVRAM.

	Command	Purpose
Step 22	Switch# **copy system:running-config tftp:**	Saves the configuration to a TFTP server. (Optional)
Step 23	Switch# **configure terminal** Switch(config)#	Enters global configuration mode.
Step 24	Switch(config)# **redundancy** Switch(config-red)#	Enters redundancy configuration mode.
Step 25	Switch(config-red)# **maintenance-mode**	Disables database autosynchronization between the CPU switch modules and puts the standby CPU switch module in cold-standby state.
Step 26	Switch(config-red)# **end** Switch#	Returns to privileged EXEC mode.
Step 27	Switch# **redundancy reload peer**	Initiates a reload of the system image on the standby CPU switch module.
Step 28	Switch# **show redundancy**	Displays the CPU switch module redundancy status and images. Verify that the standby CPU switch module is running the desired new image and is in either the NEGOTIATION state or the STANDBY COLD state.
Step 29	Switch# **redundancy switch-activity force**	Switches system control over to the standby CPU switch module by reloading the system image on the active CPU switch module.

Updating Functional Images

You can load functional images used by certain hardware controllers in the Cisco ONS 15530. This section describes the function and maintenance of functional image.

Understanding Functional Images

Functional images provide the low-level operating functionality for various hardware controllers. On hardware controllers with insystem programmable devices, such as field programmable gate arrays (FPGAs) and Erasable Programmable Logic Devices (EPLDs), the hardware functional images can be reprogrammed independently of loading the system image and without removing the devices from the controller.

On the Cisco ONS 15530, you can reprogram the functional images on the CPU switch modules, ROMMON, modules, and line cards.

All new hardware is shipped with functional images preloaded. Loading a different functional image is required only when upgrading or downgrading functional image versions.

Updating a CPU Switch Module Functional Image Release

The CPU switch modules on the Cisco ONS 15530 have two functional images, a ROMMON image and an FPGA image.

To update a CPU switch module functional images for the active and redundant CPU switch modules, follow these steps:

Step 1 Determine the release version of the CPU switch module functional image.

Step 2 Check the available space on Flash memory (bootflash or disk0) on the active CPU switch module. Make space available, if necessary.

Step 3 Copy the CPU switch module functional image to Flash memory on the standby CPU switch module.

Step 4 Load the CPU switch module functional image from Flash memory to the standby CPU switch module.

Step 5 Repeat Step 2 through Step 4 on the redundant CPU switch module after a switchover.

Note You can manage CPU switch module functional image files like any other image file on the Cisco ONS 15530. For more information on downloading and managing image files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.1*.

Caution Do not interrupt the reprogramming process. A failure during reprogramming can result in the CPU switch module being unusable. The CPU switch module functional image cannot be reverted once reprogramming starts.

Determining the CPU Switch Module Functional Image Release Version

To determine the existing CPU switch module functional image or CPU switch module functional image release version, use the following command in EXEC mode:

Command	Purpose
show hardware linecard *slot*	Displays the functional image information.
show version	Displays the ROMMON image information.

Example

The following example shows the ROMMON image version information:

```
Switch# show version

  Cisco Internetwork Operating System Software
  IOS (tm) ONS-15530 Software (ONS15530-i-mz), Release Version 12.1(10)EV2
  Copyright (c) 1986-2001 by cisco Systems, Inc.
  Compiled Fri 23-Mar-02 15:23 by
  Image text-base:0x60010950, data-base:0x604E8000

➔ ROM:System Bootstrap, Version 12.1(12c)E1, RELEASE SOFTWARE

  Switch uptime is 30 minutes
  System returned to ROM by power-on
  System image file is "disk0:ONS15530-m0-mz"

  cisco  (QUEENS-CPU) processor with 98304K/32768K bytes of memory.
  R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

  Last reset from power-on
  2 Ethernet/IEEE 802.3 interface(s)
  509K bytes of non-volatile configuration memory.

  20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
  16384K bytes of Flash internal SIMM (Sector size 64K).
  Configuration register is 0x102
```

he following example shows the functional image version for the CPU switch module in slot 5:

```
Switch# show hardware linecard 5
---------------------------------------------------------------------
Slot Number              : 5/*
Controller Type          : 0x1100
On-Board Description     : Prote-Hampton_CPU
Orderable Product Number: PROTO-HAMPTON-CPU
Board Part Number        : 73-6572-04
Board Revision           : 06
Serial Number            : CAB0602M9XX
Manufacturing Date       : mm/dd/2001
Hardware Version         : 4.6
RMA Number               :
RMA Failure Code         :
➔ Functional Image Version: 1.41 (dec), 1.29 (hex)
```

Updating a CPU Switch Module Functional Image from a TFTP Server

To download a CPU switch module functional image from a TFTP server and upgrade the functional image on both CPU switch modules, perform the following steps, starting with the active CPU switch module:

	Command	Purpose
Step 1	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory on the active CPU switch module. If space is available, continue to Step 4.
Step 2	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 3	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.

	Command	Purpose
Step 4	Switch# **copy tftp:**[[[//*location*]/*directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the TFTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.
Step 5	Switch# **show** {**sby-bootflash:** | **sby-disk0:**}	Verifies that space is available in Flash memory on the standby CPU switch module. If space is available, continue to Step 8.
Step 6	Switch# **delete** {**sby-bootflash:** | **sby-disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 7	Switch# **squeeze sby-bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 8	Switch# **copy tftp:**[[[//*location*]/*directory*]/*filename*] {**sby-bootflash:** | **sby-disk0:**}[*filename*]	Copies the image from the TFTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.
Step 9	Switch# **reprogram** {**sby-bootflash:** | **sby-disk0:**}*filename* {*slot* | **sby-rommon**}	Updates the CPU switch module functional image on the CPU switch module and returns the CPU switch module to ROMMON mode.
Step 10	rommon 1 > **boot** [{**bootflash:** | **disk0:**}*filename*]	(Optional) Boots the IOS system image on the standby CPU switch module if it does not boot automatically.
Step 11	Switch# **redundancy switch-activity** [**force**]	Switches over control to the standby CPU switch module. Repeat Step 9 through Step 10 on the new standby CPU switch module.

Note For Cisco ONS 15530 systems with only one CPU switch module, you must either power cycle the shelf or remove and reinsert the CPU switch module for the functional image upgrade to take effect.

Example

The following example shows how to download a ROMMON image from a TFTP server and update the ROMMON image on the active CPU switch module:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy tftp: disk0:
Address or name of remote host []? 10.0.0.1
Source filename []? ONS15530_RM.srec
Destination filename [ONS15530_RM.srec]? y

Loading tftpboot/ONS15530_RM.srec from 10.0.0.1 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 629458/17912748 bytes]

629458 bytes copied
```

Updating a CPU Switch Module Functional Image from an FTP Server

To download a CPU switch module functional image from an FTP server and upgrade the functional image on both CPU switch modules, perform the following steps, starting with the active CPU switch module:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	(Optional) Enters configuration mode from the terminal. This step is required only if you override the default remote username (see Step 2 and Step 3). Otherwise, continue to Step 9.
Step 2	Switch(config)# **ip ftp username** *username*	(Optional) Changes the default remote username.
Step 3	Switch(config)# **ip ftp password** *password*	(Optional) Changes the default password.
Step 4	Switch(config)# **end** Switch#	(Optional) Exits configuration mode. This step is required only if you override the default remote username (see Step 2 and Step 3).
Step 5	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory on the active CPU switch module. If space is available, continue to Step 8.
Step 6	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 7	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.

	Command	Purpose
Step 8	Switch# **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the FTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.
Step 9	Switch# **show** {**sby-bootflash:** | **sby-disk0:**}	Verifies that space is available in Flash memory on the standby CPU switch module. If space is available, continue to Step 12.
Step 10	Switch# **delete** {**sby-bootflash:** | **sby-disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 11	Switch# **squeeze sby-bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 12	Switch# **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] {**sby-bootflash:** | **sby-disk0:**}[*filename*]	Copies the image from the FTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.
Step 13	Switch# **reprogram** {**sby-bootflash:** | **sby-disk0:**}*filename* {*slot* | **sby-rommon**}	Updates the functional image on the standby CPU switch module and returns the standby CPU switch module to ROMMON mode.
Step 14	rommon 1 > **boot** [{**bootflash:** | **disk0:**}*filename*]	(Optional) Boots the IOS system image on the standby CPU switch module if it does not boot automatically.
Step 15	Switch# **redundancy switch-activity** [**force**]	Switches over control to the standby CPU switch module. Repeat Step 13 through Step 14 on the new standby CPU switch module.

Note For Cisco ONS 15530 systems with only one CPU switch module, you must either power cycle the shelf or remove and reinsert the CPU switch module for the functional image upgrade to take affect.

Example

The following example shows how to download a ROMMON image from an FTP server and update the ROMMON image on the active CPU switch module:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy ftp://myuser:mypass@theserver/tftpboot/ONS15530_RM.srec
disk0:ONS15530_RM.srec

Accessing ftp://theserver/tftpboot/ONS15530_RM.srec...Translating "theserver"...domain
server (192.168.2.132) [OK]

Loading ONS15530_RM.srec from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 623492/17912748 bytes]

623492 bytes copied
```

Updating Line Card Functional Images

You can udpate the functional image for the following line cards:

- Transponder line cards
- ESCON multiplexing line cards
- 10-Gbps ITU trunk cards
- 10-GE uplink cards
- Carrier motherboards

Update a line card functional image in three steps:

Step 1 Determine the line card functional image version.

Step 2 Copy the image to Flash memory (bootflash or disk0).

Step 3 Load the image from Flash memory to the hardware controller.

Determining the Line Card Functional Image Version

To determine the functional image version in a line card hardware controller, use the following command in privileged EXEC mode:

Command	Purpose
show hardware linecard *slot*	Displays the functional image information.

The following example shows the functional image information in the controller for the line card in slot 3:

```
Switch# show hardware linecard 3
-------------------------------------------------------------------------------
Slot Number             : 3/*
Controller Type         : 0x1101
On-Board Description    : HAMPTON-ESCON
Orderable Product Number: PROTO-HAMPTON-ESCON
Board Part Number       : 73-7710-03
Board Revision          : 01
Serial Number           : CAB0602M9PV
Manufacturing Date      : 04/08/2002
Hardware Version        : 3.2
RMA Number              :
RMA Failure Code        :
Functional Image Version: 2.36 (dec), 2.24 (hex)
```

Copying a Line Card Functional Image from a TFTP Server to Flash Memory

To download a line card functional image from a TFTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory on the active CPU switch module. If space is available, continue to Step 3.
Step 2	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 3	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 4	Switch# **copy tftp:**[[[//*location*]/*directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the TFTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.

Example

The following example shows how to download a functional image from a TFTP server and update the functional image on the active CPU switch module:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy tftp: disk0:
```

```
Address or name of remote host []? 10.0.0.1
Source filename []? fi-ons15530-escon.A.2-36.exo
Destination filename [fi-ons15530-escon.A.2-36.exo]? y

Loading tftpboot/ fi-ons15530-escon.A.2-36.exo from 10.0.0.1 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5779602/17912748 bytes]

5779602 bytes copied
```

Copying a Line Card Functional Image from an FTP Server to Flash Memory

To download a line card functional image from an FTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	(Optional) Enters configuration mode from the terminal. This step is required only if you override the default remote username (see Step 2 and Step 3). Otherwise, continue to Step 5.
Step 2	Switch(config)# **ip ftp username** *username*	(Optional) Changes the default remote username.
Step 3	Switch(config)# **ip ftp password** *password*	(Optional) Changes the default password.
Step 4	Switch(config)# **end** Switch#	(Optional) Exits configuration mode. This step is required only if you override the default remote username (see Step 2 and Step 3).
Step 5	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory. If space is available, continue to Step 8.
Step 6	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 7	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 8	Switch# **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the FTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.

Example

The following example shows how to download a functional image from an FTP server:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy ftp://myuser:mypass@theserver/tftpboot/fi-ons15530-escon.A.2-36.exo
disk0:fi-ons15530-escon.A.2-36.exo

Accessing ftp://theserver/tftpboot/ONS15530_RM.srec...Translating "theserver"...domain
server (192.168.2.132) [OK]

Loading ONS15530_RM.srec from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 623492/17912748 bytes]

623492 bytes copied
```

Updating the Line Card Functional Image

To update a line card functional image from a Flash memory device to a hardware controller, use the following command in privileged EXEC mode from a console session:

Command	Purpose
reprogram *device***:***filename slot*	Updates the functional image with the specified filename to a device.

The **reprogram** command checks the compatibility of the image for the selected card type before downloading the functional image.

Caution The download process impacts traffic through the line card.

Caution Do not interrupt the download process. Wait until it has finished before attempting any commands on the switch.

Example

The following example demonstrates loading the functional image fpga_image from the CompactFlash Card to the controller for the processor in slot 8.

```
Switch# reprogram disk0:fpga_image 8
```

Updating Module Functional Images

You can update the functional image for the OSC modules.

Update a module functional image in three steps:

Step 1 Determine the module functional image version.

Step 2 Copy the image to Flash memory (bootflash or disk0).

Step 3 Load the image from Flash memory to the hardware controller.

Determining the Module Functional Image Version

To determine the functional image version in a module hardware controller, use the following command in privileged EXEC mode:

Command	Purpose
show hardware linecard *slot*	Displays the functional image information.

The following example shows the functional image information in the controller for the line card in slot 2:

```
Switch# show hardware linecard 2
--------------------------------------------------------------------------------
Slot Number              : 2/*
Controller Type          : 0x1103
On-Board Description     : Prototype Hampton Oscmb
Orderable Product Number: PROTO-HAMPTON-OSCMB
Board Part Number        : 73-6838-04
Board Revision           : 01
Serial Number            : CAB0603MAJ1
Manufacturing Date       : 01/24/2002
Hardware Version         : 4.0
RMA Number               :
RMA Failure Code         :
Functional Image Version: 1.36
Function-ID              : 0
--------------------------------------------------------------------------------
Slot Number              : 2/0
Controller Type          : 0x1107
On-Board Description     : Prototype Hampton Oscdc
Orderable Product Number: PROTO-HAMPTON-OSCDC
Board Part Number        : 73-7238-03
Board Revision           : 03
Serial Number            : CAB0602MA36
Manufacturing Date       : 12/07/2001
Hardware Version         : 3.1
RMA Number               :
RMA Failure Code         :
Functional Image Version: 0.52
Function-ID              : 0
Transceiver type         : Non-pluggable Transceiver
--------------------------------------------------------------------------------
Slot Number              : 2/1
Controller Type          : 0x1107
On-Board Description     : Prototype Hampton Oscdc
Orderable Product Number: PROTO-HAMPTON-OSCDC
Board Part Number        : 73-7238-03
Board Revision           : 03
Serial Number            : CAB0602MA3H
Manufacturing Date       : 12/07/2001
Hardware Version         : 3.1
RMA Number               :
RMA Failure Code         :
Functional Image Version: 0.52
Function-ID              : 0
Transceiver type         : Non-pluggable Transceiver
```

Copying a Module Functional Image from a TFTP Server to Flash Memory

To download a module functional image from a TFTP server, perform the following steps:

	Command	Purpose
Step 1	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory on the active CPU switch module. If space is available, continue to Step 3.
Step 2	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.

	Command	Purpose
Step 3	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 4	Switch# **copy tftp:**[[[//*location*]/*directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the TFTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.

Example

The following example shows how to download a functional image from a TFTP server and update the functional image on the active CPU switch module:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy tftp: disk0:
Address or name of remote host []? 10.0.0.1
Source filename []? fi-ons15530-escon.A.2-36.exo
Destination filename [fi-ons15530-escon.A.2-36.exo]? y

Loading tftpboot/ fi-ons15530-escon.A.2-36.exo from 10.0.0.1 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5779602/17912748 bytes]

5779602 bytes copied
```

Copying a Module Functional Image from an FTP Server to Flash Memory

To download a module functional image from an FTP server, perform the following steps

:

	Command	Purpose
Step 1	Switch# **configure terminal** Switch(config)#	(Optional) Enters configuration mode from the terminal. This step is required only if you override the default remote username (see Step 2 and Step 3). Otherwise, continue to Step 5.
Step 2	Switch(config)# **ip ftp username** *username*	(Optional) Changes the default remote username.
Step 3	Switch(config)# **ip ftp password** *password*	(Optional) Changes the default password.

	Command	Purpose
Step 4	Switch(config)# **end** Switch#	(Optional) Exits configuration mode. This step is required only if you override the default remote username (see Step 2 and Step 3).
Step 5	Switch# **show** {**bootflash:** | **disk0:**}	Verifies that space is available in Flash memory. If space is available, continue to Step 8.
Step 6	Switch# **delete** {**bootflash:** | **disk0:**}*filename*	(Optional) Deletes a file from Flash memory.
Step 7	Switch# **squeeze bootflash:**	(Optional) Recovers the space in onboard Flash memory.
Step 8	Switch# **copy** **ftp:**[[[//[*username*[**:***password*]**@**]*location*]/ *directory*]/*filename*] {**bootflash:** | **disk0:**}[*filename*]	Copies the image from the FTP server to the Flash memory device. Reply to any CLI prompts for additional information or confirmation. The prompting depends on how much information you provide in the **copy** command. **Note** Wait until after the download finishes before attempting any commands on the switch. Confirm that the image download is done in binary mode and check file sizes before and after download.

Example

The following example shows how to download a functional image from an FTP server:

```
Switch# show disk0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    1BD2EA73  2A7B24   26  2652836 Feb 11 2002 18:07:41 ons15530-i-mz
2   .. config   36DC62E3  2AAC54   14    12461 Feb 11 2002 18:10:34 running-config

17912748 bytes available (2665556 bytes used)

Switch# copy ftp://myuser:mypass@theserver/tftpboot/fi-ons15530-escon.A.2-36.exo
disk0:fi-ons15530-escon.A.2-36.exo

Accessing ftp://theserver/tftpboot/ONS15530_RM.srec...Translating "theserver"...domain
server (192.168.2.132) [OK]

Loading ONS15530_RM.srec from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 623492/17912748 bytes]

623492 bytes copied
```

Updating the Module Functional Image

To update a module functional image from a Flash memory device to a hardware controller, use the following command in privileged EXEC mode from a console session:

Command	Purpose
reprogram *device***:***filename slot subcard*	Updates the functional image with the specified filename to a device.

The **reprogram** command checks the compatibility of the image for the selected card type before downloading the functional image.

Caution The download process impacts traffic through the module.

Caution Do not interrupt the download process. Wait until it has finished before attempting any commands on the switch.

Example

The following example demonstrates loading the functional image fpga_image from the CompactFlash Card to the controller for the processor in slot 8.

```
Switch# reprogram disk0:fpga_image 2 0
```

Command Reference

This appendix describes the commands used in the Cisco ONS 15530 environment. This appendix includes the following categories of commands:

APS Commands

APS (Automatic Protection Switching) provides protection against signal failure. Use the following commands to configure and monitor APS operations.

aps clear

To clear an APS switchover request or an APS lockout request, use the **aps clear** command.

aps clear *group-name*

Syntax Description

group-name	Specifies the name of the associated pair of interfaces.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was first introduced.

Usage Guidelines

The Cisco ONS 15530 supports APS signal switchover requests from the CLI (command-line interface). These requests have priorities based on the condition of the protection signal and the existence of another switchover or lockout request. Three types of requests exist:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the signal from switching over from the working interface to the protection interface.
- Forced switchover requests—Have the next highest priority and are only prevented when an existing lockout on the protection interface or the protection signal has failed.
- Manual switchover requests—Have the lowest priority and only occur if there is no protection path lockout, a forced switchover, or the signal has failed or degraded.

Examples

The following example shows how to clear an APS request on an associated interface pair named blue.

```
Switch# aps clear blue
```

The following example shows how to clear an APS request for an associated interface pair with the default group name.

```
Switch# aps clear Wavepatch2/0/0
```

Related Commands

Command	Description
aps lockout	Prevents switchovers to the protection path.
aps switch	Requests an APS switchover.
show aps	Displays APS configuration information and status.

aps direction

To specify unidirectional or bidirectional path switching, use the **aps direction** command. To revert to the default behavior, use the **no** form of this command.

aps direction {**unidirectional** | **bidirectional**}

no aps direction

Syntax Description

unidirectional	Specifies unidirectional path switching.
bidirectional	Specifies bidirectional path switching.

Defaults

Unidirectional

Command Modes

APS configuration

Usage Guidelines

In unidirectional path switching, only the node that detects a signal failure switches over to the standby signal. The other node continues to receive its signal on the original path. In bidirectional path switching, when a node detects a signal failure it sends a message to the other node about the failure causing that node switches over. Both nodes then use the same path through the network.

Use the **aps direction** command only with splitter and y-cable line card protection configurations. Client line card protection handles switchovers in the client equipment, not in the Cisco ONS 15530.

When using bidirectional path switching, always configure the nodes so that they communicate over the same working path and the same protection path. Also, configure both nodes that support the channel with the same APS features, such as y-cable support, revertive behavior, and path switching.

Before changing the type of path switching, disable the standby interface with the **shutdown** command. After changing the type of path switching, reenable the standby interface with the **no shutdown** command.

Note Bidirectional path switching only operates on networks that support the OSC (Optical Supervisory Channel).

Note Configure bidirectional path switching on interfaces configured with Sysplex ETR or Sysplex CLO protocol encapsulation.

Examples

The following example shows how to configure bidirectional path switching in a y-cable protection configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group alpha
Switch(config-red-aps)# working transparent 2/0/0
Switch(config-red-aps)# protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
```

The following example shows how to configure bidirectional path switching in a splitter protection configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group chicago
Switch(config-red-aps)# working wavepatch 10/0/0
Switch(config-red-aps)# protection wavepatch 10/0/1
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
```

The following example shows how to change the path switching operation for a y-cable APS group from unidirectional to bidirectional.

```
Switch# show aps group alpha

APS Group alpha :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (client side y-cable)
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  created......: 14 hours, 53 minutes
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  switched chan: 0
➔ channel  ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
             : channel  request: no-request
             : transmit request: no-request
             : receive  request: no-request
  channel  ( 1): Transparent2/0/0 (ACTIVE - UP), Wave2/0 (UP)
             : channel  request: no-request
             : switchover count: 0
             : last  switchover: never

Switch# configure terminal
Switch(config)# interface transparent 4/0/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# redundancy
Switch(config-red)# associate group Denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 4/0/0
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps revertive	Configures revertive APS for y-cable line card protection.
aps timer message holddown	Modifies the APS Channel Protocol message holddown timer interval and message count value.
aps timer message max-interval	Modifies the APS Channel Protocol maximum inactivity interval timer value.
aps timer search-for-up	Modifies the minimum and maximum timer intervals on an APS timer. The system must wait for a splitter protection connection to come up when both connections are down.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the number of seconds an APS timer must wait before switching back to the preferred working signal.
aps working	Configures the working interface of an associated interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration information and status.

aps disable

To disable APS activity between an associated interface pair, use the **aps disable** command. To reenable APS activity, use the **aps enable** command.

aps disable

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Before changing the APS configuration of an associated interface pair, use this command to disable APS activity between the interfaces. When an interface pair is initially associated, APS activity is disabled.

Examples

The following example shows how to disable APS activity between associated transparent interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
```

Related Commands

Command	Description
aps enable	Enables APS activity between associated interfaces.
associate group	Creates an APS group and enters APS configuration mode.

aps enable

To enable APS activity between an associated interface pair, use the **aps enable** command. To disable APS activity, use the **aps disable** command.

aps enable

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

After changing the APS configuration of an associated interface pair, use this command to enable APS activity between the interfaces.

Examples

The following example shows how to enable APS activity between associated transparent interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group london
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
associate group	Creates an APS group and enters APS configuration mode.

aps lockout

To lock out an APS switchover to the protection path, thus preventing any further APS switchovers for any reason, including manual or forced switchovers and signal failures, use the **aps lockout** command. To remove an APS lockout request, use the **aps clear** command.

aps lockout *group-name*

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to configure APS signal switchover lockout on the protection path. This is useful when you want to prevent a switchover during shelf maintenance, or when the protection signal has degraded or failed.

A lockout only succeeds when the protection path interface is also acting as the standby interface. If the protection path interface is the active interface, use the **aps switch** command to switch the active interface role back to the working interface.

Note The APS lockout does not persist across system reloads or CPU switch module switchovers.

Examples

The following example shows how to lock out switchover to the protection path on an associated group named group1.

```
Switch# aps lockout group1
```

Related Commands

Command	Description
aps clear	Clears the APS switchover or lockout.
aps switch	Requests an APS switchover.
aps working	Configures the working interface of an associated interface pair.
show aps	Displays APS configuration information and status.

aps message-channel

To configure message channel for the Cisco ONS 15530 to send APS channel protocol messages, use the **aps message-channel** command. To revert to the default behavior, use the **no** form of this command.

aps message-channel {**auto-select** [**far-end group-name** *name*] |
inband dcc [**far-end group-name** *name*] | **ip far-end group-name** *name* **ip-address** *ip-address*
| **osc** [**far-end group-name** *name*]**}**

no aps message-channel

Syntax Description

auto-select	APS automatically selects a transport mechanism to send APS messages.
far-end group-name *name*	Specifies the APS group name for the channel at the remote node.
inband dcc	Specifies APS to use the in-band message channel for sending APS messages.
ip	Specifies APS messages are sent over IP. APS addresses the messages to a specified group name on the remote node identified by this ip address. Use this option for APS groups that terminate on a shelf in a multiple shelf node that does not support the OSC or in-band message channel.
ip-address *ip-address*	Specifies the IP address to use to send the APS channel protocol messages.
osc	APS messages are sent on the OSC.

Defaults

auto-select with no APS group name

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The APS channel protocol communicates between nodes over the OSC or over the in-band message channel ethernetdcc interface.

The **auto-select** option automatically selects the transport channel to send the APS protocol messages attempting to use the in-band message channel first and then the OSC if the in-band message channel is not available. If neither the in-band message channel nor the OSC is available for the APS group, you must configure the message channel using the **ip** option.

Note We recommend that you configure the name for the APS group on the remote node. The APS channel protocol lookup process functions more efficiently when the group name is provided.

Examples

The following example shows how to create an APS group and configure the message channel:

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group aps_group1
Switch(config-red-aps)# aps message-channel osc far-end group-name aps-group1
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection path.
aps working	Configures the working interface for an APS interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps protection

To configure the protection path interface of an APS group, use the **aps protection** command. To remove the protection path interface, use the **no** form of this command.

aps protection {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*/*port*}

no aps protection {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port* | **waveethernetphy** *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*/*port*}

Syntax Description

transparent *slot/subcard/port*	Specifies the transparent interface to use as the protection path in y-cable line card protection.
wavepatch *slot/subcard/port*	Specifies the wavepatch interface to use as the protection path in splitter protection.
waveethernetphy *slot/subcard/port*	Specifies the waveethernetphy interface to use as the protection path in switch fabric based protection.
tengigethernetphy *slot/subcard/port*	Specifies the tengigethernetphy interface to use as the protection path in switch fabric based protection.

Defaults

None

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Each interface in an associated pair has a configured role to perform: one is the *working* interface and the other is the *protection* interface. However, at any given instant, the interfaces also have a current mode of operation: *active* and *standby.* The interface that is in active mode and receives the signal may or may not be the working interface. The working interface is the *preferred* interface to receive the active signal. The protection interface is the *preferred* interface for the standby signal.

When a pair of interfaces is associated for APS protection using the **associate interface** command, the interface with the higher interface number is the protection interface by default. To override this default configuration, use the **aps protection** command.

Examples

The following example shows how to create an APS group and configure an APS protection interface:

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection path.
aps working	Configures the working interface for an APS interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps revertive

To configure revertive APS for y-cable line card protection, use the **aps revertive** command. To disable revertive APS, use the **no** form of this command.

aps revertive

no aps revertive

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

When revertive APS is configured and a switchover to the protection signal has occurred, the system automatically switches back to the preferred working signal when it becomes operational. Use the **aps timer wait-to-restore** command to control how quickly the signal reverts back to the working path.

Examples

The following example shows how to configure revertive APS on an associated transparent interface pair.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group dallas
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps revertive
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the wait-to-restore timer interval.

Command	Description
associate group	Creates an APS group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

aps switch

To request an APS switchover from the working path to the protection path, or from the protection path to the working path, use the **aps switch** command. To clear an APS switchover request, use the **aps clear** command.

aps switch *group-name* {**force** | **manual**} {**protection-to-working** | **working-to-protection**}

Syntax Description

group-name	Specifies the name of the associated pair of interfaces.
force	Causes a switchover if no lockout is in effect.
manual	Causes a switchover if the signal is good and no lockout is in effect.
protection-to-working	Causes a manual signal switchover from the protection path to the working path if the protection path signal has not failed.
working-to-protection	Causes a manual signal switchover from the working path to the protection path whether the working path signal is active or not.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The Cisco ONS 15530 supports APS switchover requests from the CLI (command-line interface). These requests have priorities based on the condition of the protection signal and the existence of other switchover requests. Three types of requests exist:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the signal from switching over from the working interface to the protection interface.
- Forced switchover requests—Have the next highest priority and are only prevented when an existing lockout on the protection interface or the protection signal has failed.
- Manual switchover requests—Have the lowest priority and only occur if there is no protection interface lockout, a forced switchover, or the signal has failed or degraded.

In summary, the priority order is:

1. Lockout
2. Signal failure on the protection path
3. Forced signal switchover
4. Signal failure on the working path

5. Signal degrade on the working or protection path
6. Manual signal switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

Note The associated group names are case sensitive and must be entered exactly as they are shown in the **show aps** command output.

Examples

The following example shows how to make a manual switchover request from the working path to the protection path for an associated interface pair named blue.

```
Switch# aps switch blue manual working-to-protection
```

The following example shows how to make a force switchover request from the working to the protection path for an associated interface pair with the default group name.

```
Switch# aps switch Wavepatch2/0/0 force protection-to-working
```

Related Commands

Command	Description
aps clear	Clears APS switchover or lockout.
aps lockout	Prevents switchover to the protection interface.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer message holddown

To modify the APS Channel Protocol holddown timer, use the **aps timer message holddown** command. To revert to the default values, use the **no** form of this command.

aps timer message holddown *milliseconds* [**count** *number*]

no aps timer message holddown

Syntax Description

milliseconds	Specifies the number of seconds to wait before sending an APS Channel Protocol message. The range is 100 to 10,000 milliseconds. The default timer interval is 5000 milliseconds (5 seconds).
count *number*	Specifies the number of messages to send to the destination node before starting the hold-down timer. The range is 2 to 10. The default message count is 2.

Defaults

See the "Syntax Description" section.

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The holddown timer prevents APS Channel Protocol message flooding over the OSC. The holddown message count allows a specified number of messages to exchange between the nodes before the holddown timer starts. For example, if the holddown message count is set to 2, the node sends and receives two messages before the timer starts. This allows the protocol to operate efficiently without affecting system performance.

Note The default values for the holddown timer and message count are sufficient for most network configurations.

Examples

The following example shows how to modify the holddown timer and count values.

```
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer message holddown 4000 count 4
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer message max-interval	Modifies the APS Channel Protocol maximum interval timer value.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer message max-interval

To modify the maximum interval for the APS Channel Protocol inactivity timer, use the **aps timer message max-interval** command. To revert to the default value, use the **no** form of this command.

aps timer message max-interval *seconds*

no aps timer message max-interval

Syntax Description

seconds	Specifies the maximum number of seconds to wait before sending an APS Channel Protocol inactivity message. The range is 1 to 120 seconds.

Defaults

15 seconds

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

To ensure that the APS Channel Protocol is still functioning between the nodes, periodic messages are sent during periods of inactivity. The maximum interval of the inactivity timer determines how often to send the inactivity messages.

Note The default value for the inactivity timer maximum interval is sufficient for most network configurations.

Examples

The following example shows how to modify the maximum interval for the inactivity timer.

```
Switch(config)# redundancy
Switch(config-red)# associate group dallas
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer message max-interval 30
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer message holddown	Modifies the APS Channel Protocol holddown timer and message count values.

Command	Description
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer search-for-up

To modify the minimum and maximum timer intervals on an APS timer for the length of time the system waits for a splitter protection connection to come up when both connections are down, use the **aps timer search-for-up** command. To revert to the default values, use the **no** form of this command.

aps timer search-for-up *min-interval max-interval*

no aps timer search-for-up

Syntax Description

min-interval	Specifies the minimum time interval to wait for a splitter protection connection to come up before checking the other signal. The range is 1 to 120 seconds.
max-interval	Specifies the maximum timer interval to wait for a splitter protection connection to come up before checking the other signal. The range is 1 to 120 seconds.

Defaults

Minimum interval: 2 seconds

Maximum interval: 32 seconds

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to modify the minimum and maximum timer intervals on an APS timer that causes the system to wait for a splitter protection connection to come up before checking the other splitter protection connection.

When both members of a splitter pair are down, the system first checks one signal for the minimum time interval. If the splitter protection connection does not come up, the system checks the other connection and doubles the time interval. This process repeats until the maximum timer interval is reached or exceeded. Checking continues at the maximum timer interval until one of the splitter protection connections becomes active.

Note The default values for the search-for-up timer are sufficient for most network configurations.

Examples

The following example shows how to modify the minimum and maximum timer intervals for how often the system switches to check the other splitter protection connection.

```
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer search-for-up 4 16
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer switchover-enable min-interval

To modify the minimum time interval between successive APS switchovers, use the **aps timer switchover min-interval** command. To revert to the default value, use the **no** form of this command.

aps timer switchover-enable min-interval *seconds*

no aps timer switchover-enable min-interval

Syntax Description

seconds	Specifies the minimum number of seconds between successive switchovers. The range is 1 to 120 seconds.

Defaults

2 seconds

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Hardware-assisted automatic switchovers when the active signal fails are controlled by the software. An automatic switchover occurs when the system detects a signal failure or signal degradation. Automatic switchovers are disabled until the switchover timer expires. The switchover timer starts upon completion of the automatic switchover. When the timer expires, the system will allow automatic switchovers only under favorable conditions. Conditions that would prevent the system from enabling automatic switchovers include:

- Loss of light on the protection signal
- Lockout request on the protection interface, either locally or on the remote system supporting the channel
- Forced protection-to-working request in effect, either locally or on the remote system supporting the channel
- Poor quality of the protection signal

When the condition is resolved, hardware-assisted automatic switchovers are enabled.

The switchover timer prevents successive automatic switchovers from occurring too quickly and risk the loss of data.

Note The default value for the switchover timer is sufficient for most network configurations.

Examples

The following example shows how to modify the minimum interval between successive signal switchovers.

```
Switch(config)# redundancy
Switch(config-red)# associate group sanfrancisco
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer switchover-enable min-interval 4
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
associate group	Creates an APS group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

aps timer wait-to-restore

To modify the number of seconds on the APS wait-to-restore timer before reverting to the preferred working signal in a y-cable protection configuration, use the **aps timer wait-to-restore** command. To return to the default value, use the **no** form of this command.

aps timer wait-to-restore *seconds*

no aps timer wait-to-restore

Syntax Description

seconds	Specifies the number of seconds the system must wait before switching to the preferred working signal. The range is 0 to 720 seconds.

Defaults

300 seconds

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command prevents oscillations when revertive switching is configured for y-cable protected and splitter protected configurations. If the preferred working signal is unstable, the wait-to-restore timer prevents possible data loss that could result from frequent switchovers.

Caution Setting the wait-to-restore timer interval to 0 seconds disables the timer.

Note The default value for the wait-to-restore timer is sufficient for most network configurations.

Examples

The following example shows how to modify the APS wait-to-restore timer.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer wait-to-restore 180
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps revertive	Enables revertive behavior for line card protection.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
associate group	Creates an APS group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

aps working

To configure the working interface of an APS group, use the **aps working** command. To remove the working interface, use the **no** form of this command.

aps working {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port* |
waveethernetphy *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*/*port*}

no aps working {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port* |
waveethernetphy *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*/*port*}

Syntax Description

transparent *slot/subcard/port*	Specifies the transparent interface to use as the working interface in y-cable line card protection.
wavepatch *slot/subcard/port*	Specifies the wavepatch interface to use as the working interface in splitter protection.
waveethernetphy *slot/subcard/port*	Specifies the waveethernetphy interface to use as the protection path in switch fabric based protection.
tengigethernetphy *slot/subcard/port*	Specifies the tengigethernetphy interface to use as the protection path in switch fabric based protection.

Defaults

None

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Each interface in an associated pair has a configured role to perform: one is the *working* interface and the other is the *protection* interface. However, at any given instant, the interfaces also have a current mode of operation: *active* and *standby*. The interface that is in active mode, and is receiving the signal, may or may not be the working interface. The working interface is the *preferred* interface to receive the active signal. The protection interface is the *preferred* interface for the standby signal.

This command persists across system reloads.

When a pair of interfaces is associated for APS protection, the interface with the lower interface number is the working interface by default. To override this default configuration, use the **aps working** command. If there is an **aps lockout** command in effect on the protection interface, it cannot become the working interface.

Examples

The following example shows how to configure a working interface on an existing APS group:

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps working transparent 4/0/0
Switch(config-red-aps)# aps protection transparent 2/0/0
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection interface.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps y-cable

To configure y-cable line card protection, use the **aps y-cable** command. To disable y-cable line card protection, use the **no** form of this command.

aps y-cable

no aps y-cable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

APS configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to ensure that only one interface of an associated transparent interface pair transmits to the client. Signal corruption occurs when both interfaces in the pair transmit to the client over the y-cable.

Caution Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Examples

The following example shows how to configure y-cable line card protection.

```
Switch(config)# redundancy
Switch(config-red)# associate group seattle
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps direction	Modifies path switching behavior.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps revertive	Enables revertive behavior for line card protection.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.

Command	Description
aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

associate group

To enter APS configuration subcommand mode and to associate interfaces for APS protection, or to modify the attributes of an existing APS group, use the **associate group** command. To remove the group, use the **no** form of this command.

aps group-*name*

no aps group *group-name*

Syntax Description

group-name	Specifies a group name for the interface pair. Group names are case sensitive and cannot have embedded blanks.

Defaults

None

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was first introduced.

Usage Guidelines

Use this command to create an APS group, or specify an existing group, and enter APS configuration mode. You can specify group names created with this command or with the **associate interface** command.

Examples

The following example shows how to select an APS group and enter APS configuration mode.

```
Switch# configure terminal
Switch#(config)# redundancy
Switch#(config-red)# associate group blue
Switch#(config-red-aps)#
```

Related Commands

Command	Description
aps clear	Clears APS switchover or lockout.
aps direction	Modifies path switching behavior.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps lockout	Prevents switchover to the protection interface.
aps revertive	Enables revertive behavior for line card protection.
aps switch	Requests an APS switchover.
aps timer message holddown	Modifies the hold-down timer for APS Channel Protocol messages.

Command	Description
aps timer message max-interval	Modifies the maximum interval timer for APS Channel Protocol messages.
aps timer search-for-up	Modifies the search-for-up timer interval.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
aps working	Configures the working interface of an associated interface pair.
aps y-cable	Enables y-cable protection.
associate interface	Associates wavepatch interfaces for APS splitter protection.
debug aps	Enables debugging of APS and APS Channel Protocol.
redundancy	Enters redundancy configuration mode.
show aps	Displays APS configuration and operation information.
show aps trace	Displays APS and APS Channel Protocol activity information.
snmp-server enable traps aps	Enables SNMP trap notifications for APS.

associate interface

To associate the wavepatch interface pairs in a slot, or in the entire shelf, for APS splitter protection using one command, use the **associate interface** command. To disable APS protection for the interfaces, use the **no** form of this command.

associate interface wavepatch */*/*working-port* **wavepatch */*/***protection-port* [**enable** | **disable**]

associate interface wavepatch *slot*/*****/*working-port* **wavepatch** *slot*/*****/*protection-port* [**enable** | **disable**]

no associate interface wavepatch */*/*working-port* **wavepatch */*/***protection-port*

no associate interface wavepatch *slot*/*****/*working-port* **wavepatch** *slot*/*****/*protection-port*

Syntax Description

wavepatch */*/*working-port*	Specifies all wavepatch interfaces on the shelf to configure as working interfaces.
wavepatch */*/*protection-port*	Specifies all wavepatch interfaces in the shelf to configure as protection interfaces.
enable	Enables activity on the associated interface pairs. (Optional)
disable	Disables activity on the associated interface pairs. This is the default state. (Optional)
wavepatch *slot*/*****/*working-port*	Specifies all wavepatch interfaces in a slot to configure as working interfaces.
wavepatch *slot*/*****/*protection-port*	Specifies all wavepatch interfaces in a slot to configure as protection interfaces.

Defaults

The default working interface for each of the interface pairs is the first interface in the command.

APS activity between the interfaces is disabled when the interface pairs are first associated.

The default group name for each of the interface pairs is the lower interface number.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to associate the interfaces for APS protection, and then enter APS configuration mode, or to change the configuration of associated pairs. Also use this command to change the association of one interface to another interface.

When associating wavepatch interfaces with wildcards, the command mode does not enter APS configuration mode as it does when associating a pair of interfaces. Changes to the default APS attribute values must be entered for interface pairs individually. See the “Examples” section.

Associating wavepatch interfaces with wildcards does not overwrite attributes configured for a specific interface pair. For example, if you configure attributes for interface pair wavepatch 3/0/0 and wavepatch 3/0/1 with the **associate group** command, a subsequent **associate interface wavepatch 3/*/0 wavepatch 3/*/1** command does not change the attributes for the specific interface pair.

When a pair of interfaces is associated for APS protection with the **associate interface** command, the interface entered first in the command is the working interface by default.

Interfaces can be associated without being physically present in the shelf.

Examples

The following example shows how to associate all the wavepatch interfaces in the shelf for splitter protection while leaving APS activity between the interfaces disabled.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate interface wavepatch */*/0 wavepatch */*/1
Switch(config-red)#
```

The following example shows how to associate all the wavepatch interfaces in slot 2 for splitter protection, while enabling APS activity between the interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate interface wavepatch 2/*/0 wavepatch 2/*/1 enable
Switch(config-red)#
```

Related Commands

Command	Description
aps clear	Clears APS switchover or lockout.
aps direction	Modifies path switching behavior.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps lockout	Prevents switchover to the protection interface.
aps switch	Requests an APS switchover.
aps timer message holddown	Modifies the hold-down timer for APS Channel Protocol messages.
aps timer message max-interval	Modifies the maximum interval timer for APS Channel Protocol messages.
aps timer search-for-up	Modifies the search-for-up timer interval.
aps working	Configures the working interface of an associated interface pair.
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
debug aps	Enables debugging of APS and APS Channel Protocol.
redundancy	Enters redundancy configuration mode.
show aps	Displays APS configuration and operation information.
show aps trace	Displays APS and APS Channel Protocol activity information.
snmp-server enable traps aps	Enables SNMP trap notifications for APS.

show aps

To display APS configuration and status information for the system, use the **show aps** command.

show aps [**detail** | **group** *name* | **interface** *interface*]

Syntax Description

detail	Displays detailed APS information for all APS groups.
interface *interface*	Displays detailed APS information for an interface.
group *name*	Displays detailed APS information for an APS group.

Defaults

Displays summary APS information

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display APS information for an interface, an APS group, or the entire shelf.

At least one interface in an associated pair must be present on the system to use the **show aps interface** command. Otherwise, use the **show aps detail** command or the **show aps group** command to display APS information for the associated interface pair.

Note The associated group names are case sensitive. To see all the group names, use the **show aps** command.

Examples

The following example shows how to display detailed APS information for all APS groups. (See Table A-1 for field descriptions.)

```
Switch# show aps detail

APS Group blue :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: client side y-cable
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 5 minutes
  auto-failover: disabled
  transmit k1k2: sf-lp, 0, 0, 1+1, uni
  receive  k1k2: sf-lp, 0, 0, 1+1, uni
  switched chan: 0
  channel   ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
               : channel  request: no-request
               : transmit request: no-request
               : receive  request: no-request
  channel   ( 1): Transparent3/0/0 (ACTIVE - UP), Wave3/0 (UP)
               : channel  request: no-request
               : switchover count: 0
               : last  switchover: never
```

Table A-1 show aps group and show aps interface Field Descriptions

Field	Description
architecture	Shows APS architecture. Only 1+1 is supported.
remote prov:	Shows the architecture provisioning for the remote node that supports the same channel. Only 1+1 is supported.
span	Shows the APS span. Only end-to-end is supported. Also indicates if y-cable is configured.
direction	Shows signal switching behavior, either unidirectional or bidirectional.
prov:	Shows the direction provisioning for the local node.
current:	Shows the current direction status for the local node.
remote prov:	Shows the direction provisioning for the remote node that supports the same channel.
revertive	Indicates whether the group is APS revertive. Only y-cable line card protection supports revertive behavior.
wtr:	Shows the wait-to-restore timer value and its current running status.
created	Shows how long ago the group was created.
aps state	Indicates whether the working and protection channels have been associated and if APS activity is enabled.
request timer	Shows attribute values for the APS Channel Protocol timers.
holddown:	Shows the APS Channel Protocol message holddown timer value.
max:	Shows the APS Channel Protocol maximum inactivity interval timer

Table A-1 show aps group and show aps interface Field Descriptions (continued)

Field	Description
count:	Shows the APS Channel Protocol message count value.
switched chan:	Shows the switched channel number.
channel (0)	Shows the configured protection channel in the group and its current status.
channel request:	Shows the current lockout or switchover request in effect, if any. Valid values are: • no-request • manual-switch • forced-switch • lockout-of-protection
transmit request:	Shows the APS Channel Protocol message being transmitted to the remote node.Valid values are: • no-request (No request pending) • do-not-revert (Revertive behavior not enabled) • reverse-request (Response to a do-not-revert or wait-to-restore request) • wait-to-restore (Wait-to-restore timer active) • sd-lp (Signal degrade) • sf-lp (Signal failure)
receive request:	Shows the APS Channel Protocol message being received from the remote node. Values are the same as the transmit request field.
channel (1)	Shows the configured working channel in the group and its current status.
switchover count:	Shows the number of times a switchover has occurred for this pair of interfaces. Zero (0) indicates that no switchover has occurred since the system was booted.
last switchover:	Shows the elapsed time since the last switchover occurred. “Never” means that no switchover has occurred since the system was booted.

The following example shows how to display APS information for an APS group with the default group name (the default working interface). (See Table A-1 for field descriptions.)

```
Switch# show aps group Wavepatch8/0/0

APS Group Wavepatch8/0/0 :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: network side splitter
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 5 minutes
  auto-failover: disabled
  transmit k1k2: sf-lp, 0, 0, 1+1, uni
  receive  k1k2: sf-lp, 0, 0, 1+1, uni
  switched chan: 0
  channel  ( 0): Wavepatch8/0/1 (STANDBY - UP)
               : channel  request: no-request
               : transmit request: no-request
               : receive  request: no-request
  channel  ( 1): Wavepatch8/0/0 (ACTIVE - UP)
               : channel  request: no-request
               : switchover count: 1
               : last  switchover: 1 hour, 0 minutes
```

The following example shows how to display APS information for a transparent interface. (See Table A-1 for field descriptions.)

```
Switch# show aps interface transparent 8/0/0

APS Group blue :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end
  prot. mode...: client side y-cable
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  aps state....: enabled (associated)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  msg-channel..: auto (up on osc)
  created......: 5 minutes
  auto-failover: disabled
  transmit k1k2: sf-lp, 0, 0, 1+1, uni
  receive  k1k2: sf-lp, 0, 0, 1+1, uni
  switched chan: 0
  channel  ( 0): Transparent10/0/0 (STANDBY - UP)
               : external request: no-request
               : transmit request: no-request
               : receive  request: no-request
  channel  ( 1): Transparent8/0/0 (STANDBY - UP)
               : external request: no-request
               : switchover count: 0
               : last switchover.: never
```

The following example shows how to display APS summary information. (See Table A-2 for field descriptions.)

```
Switch# show aps

AR :APS Role, Wk:Working, Pr:Protection
AS :APS State, Ac:Active, St:Standby
IS :Interface State, Up:Up, Dn:Down
MPL:Minimum Protection Level, SD:Signal Degrade, SF:Signal Failure
     LOL:Loss of Light, - not currently protected

Interface             AR AS IS MPL Redundant Intf        Group Name
~~~~~~~~~~~~~~~~~~~~~ ~~ ~~ ~~ ~~~ ~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~~~~~~
Wavepatch8/0/0        Wk Ac Up LOL Wavepatch8/0/1        w
Wavepatch8/0/1        Pr St Up -   Wavepatch8/0/0        w
```

Table A-2 show aps summary Field Descriptions

Field	Description
Interface	Shows the name of the interface.
AR (APS Role)	Shows the configured role for the interface, either Wk (working) or Pr (protection). Working and protection are preferred roles configured by the **associate interface** command and the **associate group** command.
AS (APS State)	Shows the APS state, either Ac (active) or St (standby). The interface currently chosen by the system to receive the channel signal is the active interface; the other interface in the associated pair is the standby.
IS (Interface State)	Shows the interface state, either Up (up) or Dn (down).
MPL (Minimum Protection Level)	Shows the minimum protection level for signal switchover. Valid values are: • SD (signal degrade) • SF (signal failure) • LOL (loss of light) • - (not currently protected)
Redundant Intf (Interface)	Shows the other interface in the APS group.
Group Name	Shows the APS group name for the interface.

Related Commands

Command	Description
aps direction	Specifies unidirectional or bidirectional path switching.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps lockout	Configures APS lockout on a protection interface.
aps revertive	Configures revertive APS for y-cable line card protection.
aps switch	Causes a manual switchover from the working interface to the protection interface or vice versa.
aps timer message holddown	Modifies the APS Channel Protocol message holddown timer interval and message count value.

Command	Description
aps timer message max-interval	Modifies the APS Channel Protocol maximum inactivity interval timer value.
aps timer search-for-up	Modifies the minimum and maximum timer intervals on an APS timer that the system must wait for a splitter protection connection to come up when both connections are down.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the number of seconds an APS timer must wait before switching back to the preferred working signal.
aps working	Explicitly configures the working interface of an associated interface pair.
aps y-cable	Configures y-cable line card protection.
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
associate interface	Associates wavepatch interfaces for APS splitter protection.
show aps trace	Shows APS and APS Channel Protocol activity information.

show aps trace

To display APS and APS Channel Protocol activity information in the system memory, use the **show aps trace** command.

show aps trace [**clear** | **stop** | **resume | filter** *value* **| last** *number* | **detail** {**on** | **off**}]

Syntax Description

clear	Clears the APS activity trace table in memory.
stop	Stops the collection of APS activity information.
resume	Resumes the collection of APS activity information.
filter *value*	Displays only those entries that match the *value* argument.
last *number*	Displays the last number of entries indicated in the *number* argument.
detail {**on** | **off**}	Enables and disables the generation of detailed output.

Defaults

Displays all APS and APS Channel Protocol activity information in memory.

Trace is active.

Detailed output generation is disabled.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

APS trace information is similar to **show aps** command output except that it is stored in processor memory. The trace buffer contains activity information for APS and for the APS Channel Protocol.

The trace collection status and information are not saved across system or CPU switch module reloads. After the reload, the trace status returns to the default active state and the trace buffer in memory is cleared.

Examples

The following example shows how to clear the APS trace buffer:

```
Switch# show aps trace clear
```

The following example shows how to stop the APS trace activity information collection:

```
Switch# show aps trace stop
```

The following example shows how to resume the APS trace activity information collection:

```
Switch# show aps trace resume
```

The following example shows how to display detailed APS information for all APS groups. (See Table A-3 for field descriptions.)

```
Switch# show aps trace
3163.496 APS: Portgroup1/0/0: if_active
3163.496 APS: Portgroup3/0/0: if_active
3163.504 APS: Portgroup9/0/0: if_active
3164.140 ACP: lc: transmit request: (SF-LP, 0, 0, 1+1, B, 216) on DCC
3175.600 APS: WaveEthernetPhy10/0: state change (4): systeminit_flag TRUE
3175.600 APS: lc: xconnect ACTIVE  for channel 1
3175.600 APS: lc: xconnect DORMANT for channel 0
3175.600 APS: lc: state W_UP_P_UP
3175.600 APS: lc: active_red_standby
3175.600 APS: lc: work_active_red_prot_standby
3175.604 APS: lc: notify CM: assn state 3: activate channel 1
3175.604 APS: WaveEthernetPhy10/0: if_standby
3175.604 APS: WaveEthernetPhy8/0: if_active
3175.604 APS: WaveEthernetPhy8/0: lcp line active action
3175.604 APS: lc: sync state with hw, W active, P standby, caller 604E8960
3175.604 APS: lc: start hwfov_enable timer
3175.604 ACP: lc: local request: (NR, 0), caller 604EF3D4
3175.604 ACP: lc: transmit request: (NR, 0, 0, 1+1, B, 217) on DCC
3177.604 APS: lc: hwfov_enable timer expired
3177.604 APS: lc: enable auto-failover
3204.832 ACP: lc: transmit request: (NR, 0, 0, 1+1, B, 218) on DCC
3233.616 ACP: lc: transmit request: (NR, 0, 0, 1+1, B, 219) on DCC
3263.552 ACP: lc: transmit request: (NR, 0, 0, 1+1, B, 220) on DCC
```

Table A-3 show aps trace Field Descriptions

Field	Description
APS:	Specifies APS activity.
ACP:	Specifies APS Channel Protocol activity.

Related Commands

Command	Description
associate interface	Associates two interfaces for APS protection.
debug aps	Enables debugging of APS and APS Channel Protocol.
show aps	Shows APS configuration and status information.

Debug Commands

Use the following commands to debug the Cisco ONS 15530. For information on other debug commands refer to the *Cisco IOS Debug Command Reference* document.

debug aps

To debug APS operation, use the **debug aps** command. To disable APS debugging, use the **no** form of this command.

debug aps

no debug aps

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

To turn off all debugging, use the **undebug all** command.

Examples

The following example shows how to enable debugging of APS operations.

```
Switch# debug aps
```

Related Commands

Command	Description
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
associate interface	Associates wavepatch interfaces for APS splitter protection.
undebug all	Disables all debugging.

debug cdl defect-indication

To enable debugging for the in-band message channel, use the **debug cdl defect-indication** command. To disable debugging for online diagnostics, use the **no** form of this command.

debug cdl defect-indication {**error** | **events** | **periodic**}

no debug cdl defect-indication {**error** | **events** | **periodic**}

Syntax Description

error	Enables debugging for in-band message channel error conditions.
events	Enables debugging for in-band message channel internal software event conditions.
periodic	Enables debugging for in-band message channel periodic events.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable debugging for the message channel.

To turn off all debugging, use the **no debug cm** command.

Examples

The following example shows how to enable debugging of background tests for the message channel.

```
Switch# debug cm
```

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for a specified slot number.

debug cm

To enable debugging for the connection manager, use the **debug cm** command. To disable debugging for the connection manager, use the **no** form of this command.

debug cm {**errors** | **events** | **sync** {**errors** | **events**}}

no debug cm {**errors** | **events** | **sync** {**errors** | **events**}}

Syntax Description

errors	Enables debugging for message channel error conditions.
events	Enables debugging for internal software event conditions.
sync {**errors** | **events**}	Enables debugging for synchronization errors and events.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable debugging for the connection manager.

To turn off all debugging, use the **no debug cm** command.

Examples

The following example shows how to enable debugging of the connection manager.

```
Switch# debug cm events
```

Related Commands

Command	Description
undebug all	Disables all debugging.

debug cpu

To debug IPC (interprocess communication) initialization and switchover events, use the **debug cpu** command. To disable debugging IPC initialization and switchover events, use the **no** form of this command.

debug cpu {**ipc** | **redundancy** | **ehsa** | **sub-ipc**}

no debug cpu {**ipc** | **redundancy** | **ehsa** | **sub-ipc**}

Syntax Description

ipc	Enables debugging for processor IPC (interprocessor communications) initialization and switchover events.
redundancy	Enables debugging for CPU switch module redundancy initialization and operation.
ehsa	Enables debugging for processor EHSA (enhanced high system availability) services such as host name, config register, and calendar synchronizing to the standby CPU switch module.
sub-ipc	Enables debugging for the IPC channel layer below the IPC level.

Defaults

Disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable debugging of IPC initialization and switchover events. To debug redundancy software operations, use the **debug redundancy** command.

To turn off all debugging, use the **undebug all** command.

Examples

The following example shows how to enable redundancy state debugging.

```
Switch# debug cpu redundancy
```

Related Commands

Command	Description
debug redundancy	Enables debugging of redundancy software operation.
undebug all	Disables all debugging.

debug diag online

To enable debugging for online diagnostics, use the **debug diag online** command. To disable debugging for online diagnostics, use the **no** form of this command.

debug diag online [**online-insertion-removal** | **background** | **redundancy**]

no debug diag online [**online-insertion-removal** | **background** | **redundancy**]

Syntax Description

online-insertion-removal	Enables debugging of OIR (online insertion and removal) tests for online diagnostics.
background	Enables debugging of background tests for online diagnostics.
redundancy	Enables debugging of redundancy tests for online diagnostics.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable debugging for online diagnostics.

To turn off all debugging, use the **undebug all** command.

Examples

The following example shows how to enable debugging of background tests for online diagnostics.

```
Switch# debug diag online background
```

debug driver control ethernet

To enable backplane Ethernet driver debugging, use the **debug driver control ethernet** command. To disable backplane ethernet driver debugging operations, use the **no** form of this command.

debug driver control ethernet {**errors** | **events** | **packets**}

no debug driver control ethernet {**errors** | **events** | **packets**}

Syntax Description

errors	Enables debugging for SRC driver error conditions.
events	Enables debugging for internal software error conditions.
packets	Enable debugging of the backplane Ethernet drive packets.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate backplane Ethernet driver debugging.

Examples

The following example shows how to activate backplane Ethernet driver error debugging.

```
Switch# debug driver control ethernet errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver escon

To enable ESCON multiplexing line car d driver debugging, use the **debug driver escon** command. To disable ESCON multiplexing line car d driver debugging operations, use the **no** form of this command.

debug driver nvram {**errors** | **events** | **fpga**}

no debug driver nvram {**errors** | **events** | **fpga**}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for internal software events.
fpga	Enable debugging FPGA operations.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable NVRAM File system platform specific debugging.

Examples

The following example shows how to activate ESCON multiplexing line card driver debugging.

```
Switch# debug driver escon errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver nvram

To enable Cisco ONS 15530 NVRAM file system debugging, use the **debug driver nvram** command. To disable Cisco ONS 15530 NVRAM file system debugging operations, use the **no** form of this command.

debug driver nvram {**errors** | **events**}

no debug driver nvram {**errors** | **events**}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for internal software events.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable NVRAM file system platform specific debugging.

Examples

The following example shows how to activate NVRAM file system platform specific debugging.

```
Switch# debug driver nvram errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver osc

To enable the OSC driver debugging, use the **debug driver osc** command. To disable the OSC driver debugging, use the **no** form of this command.

debug driver osc {**events** | **fpga**}

no debug driver osc {**events** | **fpga**}

Syntax Description

events	Enables debugging for internal software error conditions.
fpga	Enable debugging of the FPGA.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate the OSC driver debugging.

Examples

The following example shows how to activate the OSC driver error debugging.

```
Switch# debug driver OSC errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver src

To enable SRC driver debugging, use the **debug driver src** command. To disable SRC driver debugging operations, use the **no** form of this command.

debug driver src {**errors** | **events** | **poll-errors** | **portfail** | **defect-indication** {**errors** | **events** | **periodic**}}

no debug driver src {**error** | **events** | **poll-errors** | **portfail** | **defect-indication** {**errors** | **events** | **periodic**}}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for SRC driver events.
poll-errors	Enables debugging for internal software error conditions.
portfail	Enables debugging for port failures.
defect-indication {**errors** | **events** | **periodic**}	Enables debugging for defect indications

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate SRC driver debugging.

Examples

The following example shows how to activate SRC driver debugging.

```
Switch# debug driver src
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver ten-gigabit trunk

To enable 10-Gbps ITU trunk card driver debugging, use the **debug driver ten-gigabit trunk** command. To disable 10-Gbps ITU trunk card driver debugging operations, use the **no** form of this command.

debug driver ten-gigabit trunk {**errors** | **events**}

no debug driver ten-gigabit trunk {**error** | **events**}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for SRC driver events.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate 10-Gbps ITU trunk card driver debugging.

Examples

The following example shows how to activate 10-Gbps ITU trunk card driver debugging.

```
Switch# debug driver ten-gigabit trunk events
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver voa

To enable VOA (variable optical attenuator) module driver debugging, use the **debug driver voa** command. To disable VOA module driver debugging operations, use the **no** form of this command.

debug driver voa

no debug driver voa

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate VOA module driver debugging.

Examples

The following example shows how to activate VOA module driver debugging.

```
Switch# debug driver voa
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug oscp

To debug OSCP operations, use the **debug oscp** command. To disable debugging for OSCP operations, use the **no** form of this command.

debug oscp {**events** | **hello-packet** | **transport**} [**wave** *slot*/*subcard*]

no debug oscp {**events** | **hello-packet** | **transport**} [**wave** *slot*/*subcard*]

Syntax Description

events	Enables debugging for OSCP events.
hello-packet	Enables printing of the information contained in the OSCP Hello packets.
transport	Enables debugging for OSCP transport services.
wave *slot*	Specifies the OSC interface on which to enable debugging. (Optional)

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable debugging for OSCP activity.

To disable all debugging, use the **undebug all** command.

Caution This command can generate a significant amount of output and may interfere with other activity on the system once the command is invoked.

Examples

The following example shows how to enable debugging for OSCP events.

```
Switch# debug oscp events
01:53:59:Control interface Wave1 is going up
01:54:00:OSCP:Adding neighbor on wave Wave1
```

The following example shows how to display information contained in the OSCP Hello packets.

```
Switch#

hello-packet wave 0
01:53:08:OSCP:Hello at Wave1 Tx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello at Wave1 Rx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello event 2wayd
```

Related Commands

Command	Description
show oscp info	Displays OSCP configuration information.
show oscp neighbor	Displays OSCP neighbor information.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.
undebug all	Disables all debugging.

debug ports

To debug port operations, use the **debug ports** command. To disable debugging for port operations, use the **no** form of this command.

debug ports {**connect** | **errors** [*type slot*[/*subcard*[/*port*]]] | **events** [*type slot*[/*subcard*[/*port*]]] | **patch**}

no debug ports {**connect** | **errors** [*type slot*[/*subcard*[/*port*]]] | **events** [*type slot*[/*subcard*[/*port*]]] | **patch**}

Syntax Description

connect	Enables debugging for cross connection.
errors	Enables debugging for internal software error conditions.
type slot[/*subcard*[/*port*]]	Specifies an interface on which debugging is enabled. Valid *type* values are **filter**, **filterband**, **filtergroup**, **tengigthernetphy, thru**, **transparent**, **wave**, **waveethernetphy, wavepatch**, and **wdm**. (Optional)
events	Enables debugging for internal software event conditions.
patch	Enables debugging for patch connections.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to debug common software errors and events, patch connection activity, and cross connection activity. If the interface option is not specified, debugging is enabled for all interfaces.

To disable all debugging, use the **undebug all** command.

Examples

The following example shows how to enable error debugging for transparent interface 2/0/0.

```
Switch# debug ports errors transparent 2/0/0
```

Related Commands

Command	Description
clock rate	Configures a clock rate on a transparent interface.
encapsulation	Configures the encapsulation of the client signal on the transparent interface.

Command	Description
monitor enable	Enables signal monitoring for certain protocol encapsulations.
patch	Configures patch connections for a shelf.
show connect	Displays optical connection information.
show interfaces	Displays interface information.
show patch	Displays optical patch connection configuration.
undebug all	Disables all debugging.

debug redundancy

To debug redundancy operations, use the **debug redundancy** command. To disable debugging for redundancy operations, use the **no** form of this command.

debug redundancy {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

no debug redundancy {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

Syntax Description

ehsa	Enables debugging for early software initialization suspend points associated with EHSA (enhanced high system availability).
errors	Enables debugging for redundancy internal software error conditions.
fsm	Enables debugging for redundancy finite state machine transition events.
kpa	Enables debugging for redundancy keepalive messaging events.
msg	Enables debugging for general redundancy messaging software.
progression	Enables debugging for redundancy internal state progression software.
status	Enables debugging for redundancy internal status notification software.
timer	Enables debugging for redundancy internal timers.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to debug redundancy software operations. Use the **debug cpu** command to debug CPU switch module redundancy.

To disable all debugging, use the **undebug all** command.

⚠ **Caution** This command can generate a significant amount of output and may interfere with other activity on the system once the command is invoked.

Examples

The following example shows how to debug finite state machine transition events.

```
Switch# debug redundancy fsm
```

Related Commands

Command	Description
debug cpu	Enables debugging of CPU switch module redundancy.
show redundancy	Displays CPU switch module redundancy status and configuration information.
undebug all	Disables all debugging.

debug switch

To enable switch driver debugging, use the **debug switch** command. To disable debugging switch driver operations, use the **no** form of this command.

debug switch {**errors** | **events** | **sync**}

no debug switch {**errors** | **events** | **sync**}

Syntax Description

errors	Enables debugging for switch driver error conditions.
events	Enables debugging for switch driver event conditions.
sync	Enables debugging for switch driver connections.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate switch driver debugging.

Examples

The following example shows how to enable switch fabric error debugging.

```
Switch# debug switch errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug topology

To enable topology neighbor debugging, use the **debug topology** command.

To disable debugging for redundancy operations, use the **no** form of this command.

debug topology {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

no debug topology {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

Syntax Description

ehsa	Enables debugging for early software initialization suspend points associated with EHSA (enhanced high system availability).
errors	Enables debugging for redundancy internal software error conditions.
fsm	Enables debugging for redundancy finite state machine transition events.
kpa	Enables debugging for redundancy keepalive messaging events.
msg	Enables debugging for general redundancy messaging software.
progression	Enables debugging for redundancy internal state progression software.
status	Enables debugging for redundancy internal status notification software.
timer	Enables debugging for redundancy internal timers.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to activate topology neighbor debugging.

Examples

The following example shows how to enable topology debugging.

```
Switch# debug topology
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.

Command	Description
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

undebug all

To disable all debugging, use the **undebug all** command.

undebug all

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to turn off all debugging.

Examples

The following example shows how to turn off all debugging.

```
Switch# undebug all
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug driver voa	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

Interface Configuration Commands

Use the following commands to configure and monitor the interfaces on the Cisco ONS 15530.

cdl defect-indication force hop-endpoint

To configure an interface as an end-of-hop, use the **cdl defect-indication force hop-endpoint** command. To disable end-of-hop configuration on an interface, use the **no** form of this command.

cdl defect-indication force hop-endpoint

no cdl defect-indication force hop-endpoint

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to configure the interface as a hop end point for inband message channel defect indications.

Examples

The following example shows how to enable hop endpoint on an interface.

```
Switch# configure terminal
Switch(config)# interface waveethernetphy 8/0
Switch(config-if)# cdl defect-indication force hop-endpoint
```

Related Commands

Command	Description
debug cdl defect-indication	Initiates debugging of defect indication on in-band message channel capable interfaces.
show cdl defect-indication	Displays defect indication information on in-band message channel capable interfaces.
show interfaces	Displays interface information.

cdl enable

To enable in-band message channel functionality on an interface, use the **cdl enable** command. To disable in-band message channel functionality, use the **no** form of this command.

cdl enable

no cdl enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Enable the in-band message channel on both interfaces supporting the signal.

Examples

The following example shows how to enable in-band message channel on an interface.

```
Switch# configure terminal
Switch(config)# interface esconphy 10/0/0
Switch(config-if)# cdl enable
```

Related Commands

Command	Description
cdl defect-indication force hop-endpoint	Configures an interface as an end-of-hop.
cdl flow identifier	Specifies the in-band message channel flow identifier value.
debug cdl defect-indication	Initiates debugging of the defect indication on in-band message channel capable interfaces.
show cdl defect-indication	Displays defect indication information on in-band message channel capable interfaces.
show interfaces	Displays interface information.

cdl flow identifier

To configure the in-band message channel flow identifier on an esconphy interface, use the **cdl flow identifier** command.

To remove the flow identifier, use the **no** form of this command.

cdl flow identifier *number*

no cdl flow identifier

Syntax Description

number	Specifies the flow identifier for the signal. The range is 0 to 254.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Configure the same in-band message channel flow identifier on both interfaces supporting the signal.

Examples

The following example shows how to configure the flow identified on an interface.

```
Switch# configure terminal
Switch(config)# interface esconphy 10/0/0
Switch(config-if)# cdl flow identifier 100
```

Related Commands

Command	Description
show interfaces	Displays interface information.

clock rate

To configure the signal clock rate without an associated protocol on a transparent interface, use the **clock rate** command. To disable the clock rate, use the **no** form of this command.

clock rate *value*

no clock rate

Syntax Description

value	Specifies the signal rate. The range is 16000 to 2500000 kHz.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

You can configure either the signal clock rate with either the **encapsulation** command or the **clock rate** command, but not both. Protocol monitoring cannot be enabled on the interface when the **clock rate** command is configured because no protocol is specified.

Table 0-4 lists the clock rates for well-known protocols supported by the transponder line card:

Table 0-4 Supported Clock Rates for Well-Known Protocols

Well-Known Protocol	Clock Rate (in kbps)
DS3	44,736
DV1[1] in ADI[2] mode	270,000
E3	34,368
ESCON	200,000
Fibre Channel (1 Gbps)	1,062,500
Fibre Channel (2 Gbps)	2,125,000
FICON (1 Gbps)	1,062,500
FICON (2 Gbps)	2,125,000
Gigabit Ethernet	1,250,000
ISC Compatibility Mode (ISC-1)	1,062,500
ISC Peer Mode (ISC-3)	2,125,000
SONET OC-1	51,840
SONET OC-3/SDH STM-1	155,520

Table 0-4 Supported Clock Rates for Well-Known Protocols (continued)

Well-Known Protocol	Clock Rate (in kbps)
SONET OC-12/SDH STM-4	622,080
SONET OC-24/SDH STM-8	933,120
SONET OC-48SDH STM-16	2,488,320

1. DV = digital video
2. ADI = Asynchronous Digital Interface

Examples

The following example shows how to configure the signal clock rate on an interface.

```
Switch# configure terminal
Switch(config)# interface transparent 10/0/0
Switch(config-if)# clock rate 125000
```

Related Commands

Command	Description
encapsulation	Specifies the protocol encapsulation for a transparent interface.
show interfaces	Displays interface information.

connect

To configure the signal cross connections through the switch fabric, use the **connect** command. To remove the cross connection configuration, use the **no** form of the command.

connect *interface1 interface2* [**override**]

no connect *interface1 interface2*

Syntax Description

interface1 interface2	Specifies the interfaces to be cross connected. See the "Usage Guidelines" section for valid interface types.
override	Changes the cross connect state from protection to provisioned.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to configure cross connections through the switch fabric.

To change the cross-connect state from protection to provisioned, use the **override** option with the **connect** command. When one of the interfaces specified in the connect command is APS protected, only one of the interfaces is specified in the connect command, but both are automatically included in the cross-connect installed in the switch fabric.

This option is useful for migration scenarios, when moving the APS protection to different interfaces without taking a data hit.

Valid cross connections between modules are:

- Portgroup interface on an ESCON (Enterprise Systems Connectivity) multiplexing line card to waveethernetphy subinterface on a 10-Gbps ITU trunk card

  portgroup *slot1*/*subcard1*/*port* **waveethernetphy** *slot2*/*subcard2***.***subinterface*

- Portgroup interface on an ESCON multiplexing line card to tengigethernetphy subinterface on a 10-GE uplink card

  portgroup *slot1*/*subcard1*/*port* **tengigethernetphy** *slot2*/*subcard2***.***subinterface*

You cannot preconfigure a cross connection. The interfaces must exist on the shelf before configuring them.

The order of the interfaces in the command does not affect the cross connect configuration. For example, configuring a cross connect with the command **connect portgroup 1/0/0 waveethernetphy 2/0.1** is equivalent to configuring a cross connect with **connect waveethernetphy 2/0.1 portgroup 1/0/0**.

Examples

The following example shows how to cross connect an ESCON multiplexing line card and a 10-Gbps ITU trunk card.

```
Switch# configure terminal
Switch(config)# connect portgroup 1/0/0 waveethernetphy 3/0.0 override
```

Related Commands

Command	Description
show connect	Displays the cross connections in the system.

encapsulation

To configure the protocol encapsulation for the client signal on a transparent interface, use the **encapsulation** command. To disable the encapsulation for the client signal, use the **no** form of this command.

encapsulation {**fastethernet** |
fddi |
gigabitethernet |
escon |
sysplex {**clo** | **etr** | **isc** {**compatibility** | **peer**}}
ficon {**1g** | **2g**}
sonet {**oc3** | **oc12** | **oc48**} |
sdh {**stm-1** | **stm-4**| **stm-16**} |
fibrechannel {**1g** | **2g**} [**ofc** {**enable** | **disable**}]}

no encapsulation

Syntax Description

fastethernet	Specifies Fast Ethernet encapsulation. The OFC (open fiber control) safety protocol is disabled.
fddi	Specifies FDDI encapsulation. OFC is disabled.
gigabitethernet	Specifies Gigabit Ethernet encapsulation. OFC is disabled.
escon	Specifies ESCON encapsulation. OFC is disabled.
sysplex	Specifies Sysplex encapsulation. **Note** This encapsulation is only supported on the multimode transponder line card.
clo	Specifies CLO (control link oscillator) timing. OFC is disabled. Forward laser control is enabled on both the transparent and wave interfaces.
etr	Specifies ETR (external time reference) timing. OFC is disabled.
isc	Specifies ISC (intersystem channel) encapsulation.
compatibility	Specifies ISC compatibility mode (ISC1) with rate of 1.0625 Gbps. OFC is enabled.
peer	Specifies ISC peer mode (ISC3) with rate of 2.1 Gbps. OFC is disabled.
ficon {**1g** | **2g**}	Specifies FICON encapsulation and rate. OFC is disabled.
sonet {**oc3** | **oc12** | **oc48**}	Specifies SONET encapsulation and rate. OFC is disabled.
sdh {**stm-1** | **stm-4** | **stm-16**}	Specifies SDH encapsulation and rate. OFC is disabled.
fibrechannel {**1g** | **2g**}	Specifies Fibre Channel encapsulation and rate.
ofc {**enable** | **disable**}	Enables or disables OFC. The default OFC state is disabled. (Optional)

Defaults

Encapsulation is disabled. See the “Syntax Description” section for the default OFC state.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to provide clocking for the client signal for specific protocols. The protocol encapsulation must be configured for the transparent interface to allow signal monitoring to be enabled with the **monitor enable** command. The following protocol encapsulation types are supported in 3R mode plus protocol monitoring:

- ESCON
- Fibre Channel (1 Gbps only)
- FICON
- Gigabit Ethernet
- ISC compatibility mode
- SDH
- SONET

The following protocol encapsulation types are supported in 3R mode without protocol monitoring:

- Fast Ethernet
- FDDI
- Fibre Channel (2 Gbps)
- ISC peer mode
- Sysplex CLO (control link oscillator)
- Sysplex ETR (external timer reference)

To specify the signal clock rate without specifying a protocol, use the **clock rate** command.

Sysplex CLO and Sysplex ETR are supported outside the nominal range of the clock rates for the Cisco ONS 15530 because of the nature of the traffic type.

Note Encapsulation cannot be changed without first disabling monitoring using the **no monitor enable** command.

Removing the encapsulation on a transparent interface with the **no encapsulation** command does not turn off the laser. To turn off the transmit laser to the client equipment, use the **shutdown** command.

Examples

The following example shows how to configure SONET encapsulation at a rate of OC-3 on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# encapsulation sonet oc3
```

Related Commands

Command	Description
clock rate	Configures a clock rate on a transparent interface.
monitor enable	Enables signal monitoring for certain protocol encapsulations.
show interfaces	Displays interface information.
shutdown	Disables an interface.

laser control forward enable

To enable forward laser control, which automatically shuts down line card lasers when a loss of light failure occurs, use the **laser control forward enable** command. To disable this feature, use the **no** form of this command.

laser control forward enable

no laser control forward

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled on esconphy interfaces

Disabled on all other interfaces

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable forward laser control on both the interfaces of a line card and on the OSC wave interfaces. If configured on a transparent interface, the client side laser of a transponder line card shuts down when the trunk side receiver detects a loss of light. If configured on the wave interface, the trunk side laser of the transponder line card shuts down when the client side receiver detects a loss of light.

Note To function correctly, configure forward laser control on both interfaces on a line card. For y-cable protection, configure forward laser control on both the transparent and wave interfaces on both transponder line cards.

Automatically shutting down the laser prevents the transmission of unreliable data. However, when the laser is shut down, fault isolation is more difficult.

This feature is convenient for configurations, such as Sysplex, where signal protection is performed in the client hardware and quick laser shutdown causes quick path switchover.

Caution Do not configure forward laser control when OFC is enabled. Combining these features interferes with the OFC protocol.

Examples

The following example shows how to enable forward laser control on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 3/0/0
Switch(config-if)# laser control forward enable
```

The following example shows how to enable forward laser control on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 2/0
Switch(config-if)# laser control forward enable
```

Related Commands

Command	Description
show interfaces	Displays interface information.

laser control safety enable

To enable laser safety control on a wave, waveethernetphy, or tengigethernetphy interface, use the **laser control safety enable** command. To disable laser safety control, use the **no** form of this command.

laser control safety enable

no laser control safety

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to automatically shut down the lasers transmitting to the trunk fiber when a loss of light failure occurs, such as a trunk fiber cut. Enable laser safety control on all wave interfaces in the shelf.

Laser safety control uses the same protocol state machine as OFC, but not the same timing. Laser safety control uses the pulse interval and pulse durations timers compliant with the ALS (automatic laser shutdown) standard (ITU-T G.664).

⚠ **Caution** Do not configure laser safety control when OFC is enabled. Combining these features interferes with the OFC safety protocol operation.

⚠ **Caution** Use this command only with line card protected configurations or unprotected configurations.

Examples

The following example shows how to enable laser safety control on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 2/0
Switch(config-if)# laser control safety enable
```

Related Commands

Command	Description
show interfaces	Displays interface information.

laser frequency

To select the desired channel frequency on a transparent transponder line card, use the **laser frequency** command. To revert to the default value, use the **no** form of the command.

laser frequency *number*

no laser frequency

Syntax Description

number	One of the two channel frequencies supported by the transponder line card.

Defaults

The lower frequency for the transponder laser

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The transponder line card can be tuned to support one of two channel frequencies.

The change from one frequency to another takes about 10 seconds. Do not expect traffic to transit the system until the frequency selection completes. Also, successive **laser frequency** commands are ignored until after the new channel frequency stabilizes.

Note This interface command is applicable only to tunable lasers that support transmission over multiple frequencies on the ITU grid. The values displayed for selection vary depending on the capabilities of the line card.

Examples

The following example shows how to select the channel frequency on a transponder line card wave interface:

```
Switch(config)# interface wave 9/0
Switch(config-if)# laser frequency 194100
```

Related Commands

Command	Description
show interfaces	Displays interface information.

laser shutdown

To turn off the laser on a module supporting the in-band message channel, use the **laser shutdown** command. To turn the laser on, use the **no** form of this command.

laser shutdown

no laser shutdown

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to explicitly shut down the laser. The interface **shutdown** command disables data traffic; however the control traffic carried over in-band message channel continues to flow. Use this command to turn off the laser and stop all traffic.

Note The interface **shutdown** command must precede the **laser shutdown** command. To bring the interface administratively up, the **no laser shutdown** must precede the **no shutdown** command.

Note If you turn off the laser on an interface and save the configuration to the startup configuration, the interface comes up with the laser turned off when the system boots.

Note A 10-Gbps laser on a waveethernetphy interface must warm up for 2 minutes before carrying traffic.

Examples

The following example shows how to turn off the laser on a waveethernetphy interface.

```
Switch(config)# interface waveethernetphy 4/0
Switch(config-if)# laser shutdown
```

Related Commands

Command	Description
show interfaces	Displays interface information.

loopback

To configure a signal loopback on an interface, use the **loopback** command. To disable interface loopback, use the **no** form of this command.

loopback

no loopback

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to configure line loopbacks on transparent and wave interfaces, and internal loopbacks on waveethernetphy, or tengigethernetphy interfaces. On a transponder line card, you can configure a loopback on either the wave interface or the transparent interface, but not both simultaneously.

A configured loopback differs from an external loopback where you simply run a cable from the output of a given interface to its input. Using the **loopback** command, you can set loopbacks *without* the need to change the cabling. This is useful for remote testing, configuration, and troubleshooting.

Caution Loopbacks on waveethernetphy and tengigethernetphy interfaces disrupt service. Use this feature with care.

Note If you enable loopback on an interface and save the configuration to NVRAM, the interface comes up with loopback enabled when the system boots.

Examples

The following example shows how to enable loopback on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# loopback
```

The following example shows how to enable loopback on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 10/0
Switch(config-if)# loopback
```

Related Commands

Command	Description
show interfaces	Displays interface information.

monitor enable

To monitor signal quality and protocol error statistics in the transponder line card, use the **monitor enable** command. To disable monitoring, use the **no** form of this command.

monitor enable

no monitor

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to collect error statistics on signal quality in the transponder line card. The following protocols can be monitored:

- ESCON
- Fibre Channel (1 Gbps only)
- FICON
- Gigabit Ethernet
- ISC compatibility mode
- SONET
- SDH

When monitoring is enabled on the transparent interface, it is automatically enabled on the corresponding wave interface.

For Gigabit Ethernet, Fibre Channel, and FICON, the Cisco ONS 15530 monitors the code violation and running disparity error count.

For SONET errors, the Cisco ONS 15530 monitors the SONET section overhead only, not the SONET line overhead. Specifically, the Cisco ONS 15530 monitors the B1 byte and the framing bytes. The system can detect the following defect conditions:

- Loss of Light
- Loss of Lock (when the clock cannot be recovered from the received data stream)
- Severely Errored Frame
- Loss of Frame

For SONET performance, the system monitors the B1 byte, which is used to compute the four SONET section layer performance monitor parameters:

- SEFS-S (section severely errored framing seconds)
- CV-S (section code violations)
- ES-S (section errored seconds)
- SES-S (section severely errored seconds)

Note Before monitoring can be enabled, you must configure protocol encapsulation for the interface using the **encapsulation** command.

Monitoring signal error statistics is useful for isolating system and network faults.

Examples

The following example shows how to monitor error counters on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# monitor enable
```

Related Commands

Command	Description
encapsulation	Configures the encapsulation of the client signal on the transparent interface.
show interfaces	Displays interface information.

optical attenuation

To set the attenuation level on a VOA (variable optical attenuator) module, use the **optical attenuation** command. To revert to the default behavior, use the **no** form of the command**.**

optical attenuation manual *value*

no optical attenuation manual

Syntax Description

manual	Specifies a manually entered attenuation value.
value	Specifies the attenuation value in 0.1 dB. The *value* range for WB-VOA modules is 17 to 300. The *value* range for single band PB-OE modules is 34 to 300. The *value* range for dual band PB-OE modules is 37 to 300.

Defaults

For single and double WB-VOA (wide-band variable optical attenuator) modules the default is 1.7 dB.

For single band PB-OE (per-band optical equalizer) modules the default is 3.4 dB.

For dual band PB-OE modules the default is 3.7 dB.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to set the optical attenuation on a VOA module.

Examples

The following example shows how to set the optical attenuation on a WB-VOA module.

```
Switch# configure terminal
Switch(config)# interface voain 7/0/0
Switch(config-if)# optical attenuation manual 100
```

The following example shows how to set the optical attenuation on a PB-OE module.

```
Switch# configure terminal
Switch(config)# interface voafilterin 7/0/0.1
Switch(config-subif)# optical attenuation manual 100
```

Related Commands

Command	Description
show interfaces	Displays interface information.

optical threshold power receive

To set the optical threshold power for alarms on an interface, use the **optical threshold power receive** command.To revert to the default values, use the **no** form of the command.

optical threshold power receive [**after-attenuation**] {**low** | **high**} {**alarm** | **warning**} *value* **[severity {critical | major | minor | not alarmed | not reported}]**

no optical threshold power receive [**after-attenuation**] {**low** | **high**} {**alarm** | **warning**}

Syntax Description

after-attenuation	Indicates that the threshold is measured after passing through a VOA (variable optical attenuator) at this interface.
low	Specifies a low threshold value.
high	Specifies a high threshold value.
alarm	Indicates that an alarm will be raised when the threshold is exceeded.
warning	Indicates that a warning indication will be reported when the threshold is exceeded.
value	The threshold value in tenths of a dBm. The range is –400 to 250.
severity	Specifies the severity for the threshold.
critical	Indicates the threshold level for service-affecting conditions that require immediate corrective action. This severity applies only to alarms.
major	Indicates the threshold level for hardware or software conditions that cause serious service disruption, or malfunctioning or failure of important hardware. These problems require the immediate attention and response of a technician to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance. This severity applies only to alarms.
minor	Indicates the threshold level for problems that do not have a serious effect on service, or for problems in hardware that do not affect the essential operation of the system. This severity applies to both alarms and warnings.
not-alarmed	Indicates the threshold level for negligible discrepancies, and that do not cause alarm notifications to be generated. The information for these events is retrievable from the network element. This severity applies only to warnings.
not reported	Indicates the threshold level for negligible discrepancies, and that do not cause notifications to be generated. The information for these events is retrievable from the network element. This severity applies only to warnings.

Defaults

Interface Type	Low Alarm	Low Warning	High Alarm	High Warning
Voafilterin subinterface	–29 dBm	–27 dBm	11 dBm	9 dBm
Voain	–29 dBm	–27 dBm	11 dBm	9 dBm

Interface Type	Low Alarm	Low Warning	High Alarm	High Warning
Active wavepatch on a 2.5-Gbps transponder line card	–28 dBm	–26 dBm	–8 dBm	–10 dBm
Standby wavepatch on a 2.5-Gbps transponder line card	–28 dBm	–26 dBm	–15 dBm	–13 dBm
Active wavepatch on a 10-Gbps transponder module	–22 dBm	–20 dBm	–6 dBm	–8 dBm

For the alarm and warning threshold default values, see the "Usage Guidelines" section.

Alarm severity: **major**

Warning severity: **not alarmed**

Command Modes

Interface configuration for WB-VOA modules, transponder line cards, and 10-Gbps ITU trunk cards

Subinterface configuration for PB-OE modules

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The default value for high alarm threshold corresponds to the receiver saturation level for the transponder module.

The default value for low alarm threshold corresponds to the Loss of Light condition. Exceeding the low alarm threshold on the active wavepatch interface causes a protection switchover to the standby wavepatch interface, provided that the standby interface is up and operating normally prior to the protection switchover.

The default values cover most network configurations. However, when optical amplifiers are used in the network in the receive direction as preamplifiers, the low alarm threshold value should be reconfigured, since the amplified noise level might be higher than the sensitivity of the receiver and the protection switchover might not be triggered. In such cases, we recommend setting the low alarm threshold to 10 dB below the power level measured at the interface when a signal exists or to –28 dB, whichever value is greater.

The value of a high warning threshold must be less than the value of the high alarm threshold. The value of a low warning threshold must be greater than the value of the low alarm threshold.

Examples

The following example shows how to set the optical power low alarm threshold on a PB-OE module.

```
Switch(config)# interface voafilterin 9/0/0.1
Switch(config-if)# optical threshold power receive after-attenuation low alarm -210
```

The following example shows how to set the optical power high alarm threshold on a WB-VOA module.

```
Switch(config)# interface voain 8/0/0
Switch(config-if)# optical threshold power receive after-attenuation high alarm -200
```

The following example shows how to set the optical power low warning threshold on a wavepatch interface.

```
Switch(config)# interface wavepatch 4/0/0
Switch(config-if)# optical threshold power receive low warning -200
```

Related Commands

Command	Description
show interfaces	Displays interface information.

patch

To configure the patch connections within a shelf, use the **patch** command. To remove the patch connection configuration, use the **no** form of the command.

patch *interface1* [**transmit** | **receive**] *interface2*

no patch *interface1* [**transmit** | **receive**] *interface2*

Syntax Description

interface1	Specifies the first patched interface. See the "Usage Guidelines" section for valid interface types.
transmit	Indicates that *interface1* is patched to *interface2* in the transmit direction.
receive	Indicates that a*interface1* is patched to *interface2* in the receive direction.
interface2	Specifies the second patched interface. See the "Usage Guidelines" section for valid interface types.

Defaults

Both directions

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to describe the patch connections between the OADM modules.

Valid patch connections between modules are:

- Thru interface to thru interface between OADM modules

  thru *slot1*/*subcard1* **thru** *slot*/*subcard2*
- OSC wave interface to OSC oscfilter interface

  wave *slot* **oscfilter** *slot*/*subcard*
- OSC oscfilter interface to OSC wave interface

  oscfilter *slot*/*subcard* **wave** *slot*
- Wavepatch interface to OADM filter interface

  wavepatch *slot*/*subcard*/*port* **filter** *slot*/*subcard*/*port*
- OADM wdm interface to WBVOA voain interface

  wdm *slot*/*subcard* **voain** *slot*/*subcard*/*port*
- OADM wdm interface to WBVOA voaout interface

  wdm *slot*/*subcard* **voaout** *slot*/*subcard*/*port*
- OADM wdm interface to PBOE voafilterin interface

wdm *slot*/*subcard* **voafilterin** *slot*/*subcard*/*port*

- OADM wdm interface to PBOE voafilterout interface

  wdm *slot*/*subcard* **voafilterout** *slot*/*subcard*/*port*
- PBOE voabypassout interface to WBVOA voa in interface

  voabypassout *slot*/*subcard*/*port* **voain** *slot*/*subcard*/*port*
- WBVOA voa out interface to PBOE voabypassin interface

  voaout *slot*/*subcard*/*port* **voabypassin** *slot*/*subcard*/*port*
- PBOE voabypassout interface to PBOE voafilter in interface

  voabypassout *slot*/*subcard*/*port* **voafilterin** *slot*/*subcard*/*port*
- PBOE voafilterout interface to PBOE voabypassin interface

  voafilterout *slot*/*subcard*/*port* **voabypassin** *slot*/*subcard*/*port*

You cannot preconfigure a patch connection. The interfaces must exist on the shelf before configuring them.

The order of the interfaces in the command does not affect the patch connect configuration. For example, configuring **patch wdm 0/1 thru 0/0** is equivalent to configuring **patch thru 0/0 wdm 0/1**.

In case of an optical interface where the transmitted and received signals travel on two different strands of fiber, it is possible that each fiber is patched to a different interface. The direction keywords **receive** and **transmit** indicate whether *interface1* is patched to the *interface2* in the receive direction or the transmit direction. The absence of the keyword indicates that *interface1* is patched to *interface2* in both directions.

When one interface in a patch connection is physically removed from the shelf, the patch connection configuration persists but does not appear in the **show running-config** output. A subsequent **patch** command that includes the remaining interface overwrites the previous patch connection configuration.

Examples

The following example shows how to describe the patch connection between two OADM modules in the same slot.

```
Switch# configure terminal
Switch(config)# patch wdm 0/0 wave 1/1
```

The following example shows how to describe the patch connection in the transmit direction between an OADM module and a PBOE module.

```
Switch# configure terminal
Switch(config)# patch wdm 1/0 transmit voafilterin 1/1/0
```

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
show optical filter	Displays the channels supported by the OADM modules.
show patch	Displays optical patch connection configuration.
snmp-server enable traps cdl	Enables SNMP trap notifications for patch connection activity.

show cdl defect-indication

To display the defect indication information on in-band message channel capable interfaces use the **show cdl defect-indication** command.

show cdl defect-indication [**interface** *interface* | **detail**]

Syntax Description

detail	Displays the defect indication information for in-band message channel capable interfaces.
interface *interface*	Displays the defect indication information for a specific interface.

Defaults

Displays a defect indication summary

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command is used to display the defect indication information on in-band message channel capable interfaces.

Examples

The following example shows how to display in-band message channel defect indication information. (See Table A-5 for field descriptions.)

```
Switch# show cdl defect-indication
CDL Defect-Indication Status Summary
Interface    Interface   DI       Defect-Indication       Defect-Indication
Name         Status     Status          Receive                Transmit
------------ ---------- ------ ----------------------- -----------------------
WaveE3/0     up         up              None                    None
WaveE4/0     up         up              None                    None
WaveE9/0     up         up              None                    None
WaveE10/0    up         up              None                    None
```

Table A-5 show cdl defect-indication Field Descriptions

Field	Description
Interface Name	Shows the interface identifier.
Interface Status	Shows the interface status.
DI Status	Shows the defect indication status.
Defect-Indication Receive	Shows the defect indication on the receive signal.
Defect-Indication Transmit	Shows the defect indication on the transmit signal.

The following example shows how to display the defect indication information for in-band message channel capable interfaces.

```
Switch# show cdl defect-indication detail

Interface WaveEthernetPhy3/0
Oper.  Status: up
Admin. Status: up
Configured Node Behavior: Hop Terminating
Current Node Behavior   : Hop Terminating
Defect Indication Receive :          None
Defect Indication Transmit:          None

Interface WaveEthernetPhy4/0
Oper.  Status: up
Admin. Status: up
Configured Node Behavior: Hop Terminating
Current Node Behavior   : Hop Terminating
Defect Indication Receive :          None
Defect Indication Transmit:          None
```

Related Commands

Command	Description
cdl defect-indication force hop-endpoint	Configures an interface as an end-of-hop.
cdl enable	Enables in-band message channel functionality.
cdl flow identifier	Specifies the in-band message channel flow identifier value.
debug cdl defect-indication	Initiates debugging of defect indication on in-band message channel capable interfaces.

show connect

To display the connection relationships between the interfaces in the shelf, use the **show connect** command.

show connect [**edges** | **intermediate** [**sort-channel** | **interface** *interface*]]

Syntax Description

edges	Displays the connections between the client (transparent) interfaces and network trunk (wdm) interfaces of the shelf.
intermediate	Displays the complete connections between the client transparent interfaces and network trunk wdm interfaces of the shelf, including all the intermediate internal interfaces.
sort-channel	Sorts the display by channel number.
interface *interface*	Displays the intermediate connection information for a specific interface.

Defaults

Summary of configured cross connections

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command shows the relationships between the interfaces in the shelf. Use this command to trace a single channel from the client side interface to the trunk side OADM interface.

Examples

The following example shows how to display configured cross connection information. (See Table A-7 for field descriptions.)

```
Switch# show connect
Index Client Intf     Trunk Intf      Kind        C2TStatus  T2CliStatus
----- --------------- --------------- ----------- ----------  ---------
15    Port3/0/0       WaveE8/0.1      Provisioned Up         Up
15    Port3/0/0       WaveE10/0.1     Protection  Up         Dormant
```

Table A-6 show connect Field Descriptions

Field	Description
Index	Shows the index value in the MIB.
Client Intf	Shows the client interface identifier.
Trunk Intf	Shows the trunk interface identifier.

Table A-6 show connect Field Descriptions (continued)

Field	Description
Kind	Indicates the kind of cross connections. The values are: • Provisioned • Protection
C2TStatus	Indicates the status of the signal from the client interface to the trunk interface.The values are: • Up • Down
T2CliStatus	Indicates the status of the signal from the trunk interface to the client interface.The values are: • Up • Dormant

The following example shows how to display edge connection information. (See Table A-7 for field descriptions.)

```
Switch# show connect edges
client/
wave        wdm  channel
----------  ---  -----
Tran4/0/0      0/1      4
```

Table A-7 show connect edges Field Descriptions

Field	Description
client/wave	Shows the client side interface identifier.
wdm	Shows the wdm interface identifier.
channel	Shows the ITU wavelength number supported by this connection.

The following example shows how to display intermediate connection information. (See Table A-8 for field descriptions.)

```
Switch# show connect intermediate
client/       wave           wave            wdm
client/       wave           wave             wdm
wave          client         patch   filter   trk  channel
------------  ------------  -------  ------  ----- -------
Esco3/0/0     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/1     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/2     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/3     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/4     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/5     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/6     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/7     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/8     WaveE8/0       8/0/0*
                             8/0/1
Esco3/0/9     WaveE8/0       8/0/0*
                             8/0/1
client/       wave           wave             wdm
wave          client         patch   filter   trk  channel
------------  ------------  -------  ------  ----- -------

Tran4/0/0     Wave4/0        4/0/0*  0/1/3    0/1    4
                             4/0/1
Tran7/0/0     Wave7/0        7/0/0
                             7/0/1*  0/0/2    0/0    3
```

Table A-8 show connect intermediate Field Descriptions

Field	Description
client/wave	Shows the client side interface identifier.
wave client	Shows the wave interface identifier.
wave patch	Shows the wavepatch interface identifier. The interface with the asterisk (*) carries the active signal.
filter	Shows the filter interface identifier.
wdm trk	Shows the wdm interface identifier.
channel	Shows the channel number supported by this connection.

The following example shows how to display interface connection information. (See Table A-9 for field descriptions.)

```
Switch# show connect interface transparent 2/0/0
client/       wave           wave                wdm
wave          client         patch   filter   trk  channel
------------  ------------  -------  ------  -----  -------
Esco3/0/0     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/1     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/2     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/3     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/4     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/5     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/6     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/7     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/8     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
Esco3/0/9     WaveE8/0.1     8/0/0*  0/0/1    0/0    2
                             8/0/1   0/1/1    0/1    2
client/       wave           wave                wdm
wave          client         patch   filter   trk  channel
------------  ------------  -------  ------  -----  -------

Tran4/0/0     Wave4/0        4/0/0*  0/1/3    0/1    4
                             4/0/1
Tran7/0/0     Wave7/0        7/0/0
                             7/0/1*  0/0/2    0/0    3
```

Table A-9 show connect interface Field Descriptions

Field	Description
Client	Shows the client side interface identifier.
Wave	Shows the wave interface identifier.
Wavepatch	Shows the wavepatch interface identifier.
Filter	Shows the filter interface identifier.
Wdm	Shows the wdm interface identifier.
Thru	Shows the thru interface identifier.
Wdm (trnk)	Shows the identifier of the wdm interface attached to the trunk fiber.

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
show optical filter	Displays information about the channels supported by the OADM modules.
show optical wavelength mapping	Displays the mapping of the Cisco ONS 15530 channels to the ITU grid wavelengths and frequencies.

show controllers

To display hardware register information for an interface, use the **show controllers** command.

show controllers [*type slot*[/*subcard*[/*port*]]]

Syntax Description

type	Specifies one of the interface types listed in Table A-10.
slot	Specifies a chassis slot.
subcard	Specifies a subcard position in a motherboard.
port	Specifies a port.

Defaults

Displays controller information for all interfaces on the system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The **show controllers** command displays the contents of hardware registers for the interfaces. This information is useful for troubleshooting system problems.

Table A-10 shows the interface types for the **show controller** command.

Table A-10 Interface Types for the show controller Command

Type	Description
fastethernet 0	Shows the NME interface information.
filter *slot/subcard/port*	Shows the filter interface information.
filterband *slot/subcard/port*	Shows the filterband interface information.
filtergroup *slot/subcard/port*	Shows the filtergroup interface information.
gigabitphy *slot/0*	Shows the Gigabitphy interface information.
oscfilter *slot/subcard*	Shows the OSC oscfilter interface information.
portgroup *slot/0/0*	Shows the portgroup interface information.
thru *slot/subcard*	Shows the thru interface information.
transparent *slot/subcard/***0**	Shows the transparent interface information.
wave *slot*[/*subcard*]	Shows the wave interface information.
waveethernitphy *slot/0*	Shows the waveethernetphy interface information.
wavepatch *slot/subcard/port*	Shows the wavepatch interface information.
wdm *slot/subcard*	Shows the wdm interface information.

Examples

The following example shows how to display hardware register information about a transparent interface. (See Table A-11 for field descriptions.)

```
Switch# show controllers transparent 3/0/0
Controller info for Transparent interface Transparent3/0/0
  LRC start addr = 0x200000
  hardware port = 1
    RCI0 monitor................:enabled
    port 1 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x0
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x0
    port error register.........:0x10000
    port ctrl msg intf mask.....:0x0
    port APS port fail mask.....:0x0
  HuJr start addr = 0x240000
  Optics control and status:
    LSC indication..............:ok
    trunk laser failure alarm...:clear
    LSC indication enable.......:disabled
    trunk laser alarm enable....:disabled
    line transceiver mode.......:non pluggable
    loss of light...............:yes
    trunk laser deviation alarm.:clear
    LSC.........................:disabled
    quick shutdown (FLC)........:disabled
    wavelength select...........:n-1 [lo wlen]
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:disabled
  SerDes control and status:
    diags loop back.............:disabled
    line loop back..............:disabled
  GE handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  FC/ESCON handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  SONET handler control and status:
    loss of frame...............:yes
    severely errored frame......:yes
    LOF enable..................:disabled
    SEF enable..................:disabled
```

Table A-11 show controllers Command Field Descriptions for Transparent Interfaces

Field	Description
Optics control and status:	Shows control and status information for the optical components in the interface.
LSC indication	Shows laser safety control status (valid only on wave interfaces).
trunk laser failure alarm	Shows the status of the trunk laser alarm. The values are: • clear—no failure • indicated—failure
LSC indication enable	Indicates whether laser safety control has been enabled (valid only on wave interfaces).

Table A-11 show controllers Command Field Descriptions for Transparent Interfaces (continued)

Field	Description
trunk laser alarm enable	Shows the status of the trunk laser alarm. If enabled, the system will signal when laser failure occurs.
loss of light	Indicate whether there is a loss of light condition.
trunk laser deviation alarm	Shows the status of the wavelength deviation alarm. If enabled, the system will signal when there is a deviation in the functioning of the laser.
LSC	Indicates whether laser safety control is enabled from the CLI (valid only on wave interfaces).
quick shutdown (FLC)	Indicates whether forward laser control is enabled on the interface (valid only on wave interfaces).
wavelength select	Indicates whether a transponder line card is transmitting the lower wavelength (lo wlen) or the higher wavelength (hi wlen).
CDR control and status:	Shows the CDR (clock and data recovery) control and status information.
loss of lock	Indicated whether there is a loss of lock condition.
loss of lock enable	Indicates whether loss of lock monitoring is enabled on the interface via the **monitor enable** command.
SerDes control and status:	Shows the SerDes (serializer/deserializer) information.
GE handler control and status:	Shows Gigabit Ethernet control and status information.
loss of sync	Indicates whether there is a loss of synchronization for the signal. This field is only valid if protocol encapsulation is Gigabit Ethernet, and monitoring is enabled.
loss of sync enable	Indicates whether loss of synchronization monitoring is enabled via the **monitor enable** command.
FC/ESCON handler control and status:	Shows Fibre Channel and ESCON control and status information.
loss of sync	Indicates whether there is a loss of synchronization for the signal. This field is only valid if protocol encapsulation is Fibre Channel or ESCON, and monitoring is enabled.
loss of sync enable	Indicates whether loss of synchronization monitoring is enabled via the **monitor enable** command.
SONET handler control and status:	Shows SONET control and status information.
loss of frame	Indicates whether there is a loss of frame for the signal. This field is only valid if protocol encapsulation is SONET, and monitoring is enabled.
severely errored frame	Indicates whether there is a severely errored frame in the signal. This field is only valid if protocol encapsulation is SONET, and monitoring is enabled.

Table A-11 show controllers Command Field Descriptions for Transparent Interfaces (continued)

Field	Description
LOF enable	Indicates whether loss of frame monitoring is enabled via the **monitor enable** command.
SEF enable	Indicates whether severely errored frame monitoring is enabled via the **monitor enable** command.

The following example shows how to display hardware register information about a transponder line card wave interface. (See Table A-11 for field descriptions.)

```
Switch# show controllers wave 3/1
Controller info for Wave interface Wave3/1
  LRC start addr = 0x200000
  hardware port = 2
    RCI1 monitor................:enabled
    port 2 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x0
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x0
    port error register.........:0x10000
    port ctrl msg intf mask.....:0xF00FC00A
    port APS port fail mask.....:0x0
  HuJr start addr = 0x250000
  Optics control and status:
    auto fail-over indication...:normal
    optical switch alarm........:clear
    line laser degrade alarm....:clear
    optical switch position.....:Mux 1
    loss of light...............:no
    BLC and LAS.................:disabled
    LSC.........................:disabled
    quick shutdown (FLC)........:disabled
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:enabled
  SerDes control and status:
    diags loop back.............:disabled
    line loop back..............:disabled
  GE handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  FC/ESCON handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  SONET handler control and status:
    loss of frame...............:yes
    severely errored frame......:yes
    LOF enable..................:disabled
    SEF enable..................:disabled
```

The following example shows how to display hardware register information about an OSC wave interface. (See Table A-11 for field descriptions.)

```
Switch# show controllers wave 3/0
Controller info for OSC wave interface Wave3/0
  LRC start addr = 0x900000
  hardware port = 0
    RCI0 monitor................:enabled
    port 0 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x1060000
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x1070000
    port error register.........:0x8002
    port ctrl msg intf mask.....:0x0
    port APS port fail mask.....:0x0
  HuJr start addr = 0x940000
  CDL add/drop control and status:
    FIFO overflow indication....:clear
    HEC error threshold exceeded:indicate
    FIFO overflow enable........:disabled
    HEC error threshold enable..:disabled
    CDL alarm status............:true alarm
    CDL add enable..............:enabled
    CDL drop enable.............:enabled
  Optics control and status:
    LSC indication..............:ok
    trunk laser failure alarm...:indicated
    LSC indication enable.......:disabled
    trunk laser alarm enable....:disabled
    loss of light...............:yes
    wavelength deviation alarm..:clear
    LSC.........................:disabled
    wavelength select...........:n [hi wlen]
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:disabled
  SerDes control and status:
    diags loop back.............:disabled
    network loop back...........:disabled
  GE handler control and status:
    loss of sync................:yes
    loss of sync enable.........:disabled
```

Related Commands

Command	Description
encapsulation	Specifies the protocol encapsulation for a transparent interface.
laser control forward enable	Configures forward laser control, which automatically shuts down transponder line card lasers.
laser control safety enable	Configures laser safety control on a wave, waveethernetphy, or tengigethernetphy interface.
loopback	Configures signal loopback on transparent and wave interfaces.
monitor enable	Enables signal monitoring for certain protocol encapsulations.
show interfaces	Displays interface information.

show interfaces

To display interface information, use the **show interfaces** command.

show interfaces [*type slot*[/*subcard*[/*port*]]]

Syntax Description

type	Specifies one of the interface types listed in Table A-12.
slot	Specifies a chassis slot.
subcard	Specifies a subcard position in a motherboard.
port	Specifies a port.

Defaults

Displays information for all interfaces on the system.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Table A-12 shows the interface types for the **show interfaces** command.

Table A-12 Interface Types for the show interfaces Command

Type	Description
esconphy *slot*/**0**/*port*	Shows the esconphy interface information.
fastethernet 0	Shows the NME interface information.
fastethernet-sby 0	Shows the NME interface information for the standby CPU switch module.
filter 0/*subcard*/*port*	Shows the filter interface information.
oscfilter *slot*/*subcard*	Shows the OSC oscfilter interface information.
portgroup *slot*/**0**	Shows the portgroup interface information.
tengigethernetphy *slot*/**0**	Shows the tengigethernetphy interface information.
tengigethernetphy *slot*/**0.***subinterface*	Shows the tengigethernetphy subinterface information.
thru 0/*subcard*	Shows the thru interface information.
transparent *slot*/**0**/**0**	Shows the transparent interface information.
voabypassin *slot*/*subcard*/**0**	Shows the voabypassin interface information.
voabypassout *slot*/*subcard*/**0**	Shows the voabypassout interface information.
voafilterin *slot*/*subcard*/**0.***subinterface*	Shows the voafilterin interface information.
voafilterout *slot*/*subcard*/**0**	Shows the voafilterout interface information.

Table A-12 Interface Types for the show interfaces Command

Type	Description
voain *slot*/*subcard*/**0.***subinterface*	Shows the voain interface information.
voaout *slot*/*subcard*/**0**	Shows the voaout interface information.
wave *slot*/**0**	Shows the wave interface information.
wavepatch *slot*/**0**/*port*	Shows the wavepatch interface information.
waveethernetphy *slot*/**0**	Shows the waveethernetphy interface information.
waveethernetphy *slot*/**0.***subinterface*	Shows the waveethernetphy subinterface information.
wdm 0/*subcard*	Shows the wdm interface information.

Examples

The following example shows how to display transparent interface information. (See Table A-13 for field descriptions.)

```
Switch# show interfaces transparent 3/0/0
Transparent3/0/0 is administratively up, line protocol is up
  Signal quality: Loss of lock
  Encapsulation: Sonet    Rate: oc3
  Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: None
  Threshold monitored for: BIP1 error
  Set threshold SF:10e-5  SD:10e-7
  Section code violation error count(bip1): 61286
  Number of errored seconds(es): 2
  Number of severely errored seconds(ses): 2
  Number of severely errored framing seconds(sefs): 273
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 2
  Loopback not set
  Last clearing of "show interface" counters never
Hardware is transparent
```

Table A-13 show interfaces transparent Field Descriptions

Field	Description
Transparent 3/0/0 is administratively up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.
Signal quality	Shows signal quality.
Encapsulation	Shows the encapsulation for the interface.
Rate	Shows the encapsulation rate—either the configured clock rate or the protocol clock rate, if the protocol supports multiple rates.
Signal monitoring	Shows whether signal monitoring is enabled.
Forward laser control	Shows whether forward laser control is enabled.
Configured threshold group	Shows whether a threshold group has been configured for the interface.
Threshold monitored for	Shows what the threshold group is monitored for.

Table A-13 show interfaces transparent Field Descriptions (continued)

Field	Description
Set threshold	Shows alarm thresholds. The output example shows the alarm thresholds for signal failure (SF) and signal degrade (SD).
Section code violation error count (bip1)	Shows the number of BIP1 errors.
Number of errored seconds (es)	Shows the number of errored seconds.
Number of severely errored seconds (ses)	Shows the number of severely errored seconds.
Number of severely errored framing seconds (sefs)	Shows the number of severely errored framing seconds.
Number of times SEF alarm raised	Shows the number of times the SEF alarm was raised.
Number of times SF threshold exceeded	Shows the number of times the signal failure (SF) threshold was exceeded.
Number of times SD threshold exceeded	Shows the number of times the signal degrade (SD) threshold was exceeded.
Loopback not set	Shows whether loopback is enabled.
Last clearing of “show interface” counters	Shows the last time “show interface” counters were cleared.
Hardware is transparent	Shows the hardware type.

The following example shows how to display wave interface information. (See Table A-14 for field descriptions.)

```
Switch# show interfaces wave 10/0
Wave10/0 is administratively up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz    Wavelength: 1536.61 nm
  Splitter Protected: Yes
  Receiver power level: -37.30 dBm
  Laser safety control: Off
  Forward laser control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Section code violation error count(bip1): 0
  Number of errored seconds(es): 29
  Number of severely errored seconds(ses): 29
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters 4d03h
  Hardware is data_only_port
```

Table A-14 show interfaces wave Field Descriptions

Field	Description
Wave10/0 is administratively up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.

Table A-14 show interfaces wave Field Descriptions (continued)

Field	Description
Channel Frequency Wavelength	Shows the channel number, frequency, and wavelength of the wave interface.
Splitter Protected	Shows whether the interface is splitter protected.
Receiver power level	Shows the receiver power level. **Note** This field is not present in the OSC wave interface output.
Laser safety control	Shows whether laser safety control is enabled.
Forward laser control	Shows whether forward laser control is enabled.
Osc physical port	Shows whether the interface is an OSC physical port.
Wavelength used for inband management	Shows whether the interface is used for inband management.
Configured threshold group	Shows whether a threshold group has been configured for the interface.
Section code violation error count (bip1)	Shows the number of BIP1 errors.
Number of errored seconds (es)	Shows the number of errored seconds.
Number of severely errored seconds (ses)	Shows the number of severely errored seconds.
Number of severely errored framing seconds (sefs)	Shows the number of severely errored framing seconds.
Number of times SEF alarm raised	Shows the number of times the SEF alarm was raised.
Number of times SF threshold exceeded	Shows the number of times the signal failure (SF) threshold was exceeded.
Number of times SD threshold exceeded	Shows the number of times the signal degrade (SD) threshold was exceeded.
Loopback not set	Shows whether loopback is enabled.
Last clearing of “show interface” counters	Shows the last time “show interface” counters were cleared.
Hardware is data_only_port	Shows the interface type.

The following example shows how to display OSC wave interface information. (See Table A-14 for field descriptions.)

```
Switch# show interfaces wave 2/0
Wave2/0 is up, line protocol is up
  Channel: 0    Frequency: 191.9 Thz    Wavelength: 1562.23 nm
  Laser safety control: Off
  Osc physical port: Yes
  Wavelength used for inband management: No
  Configured threshold Group: None
  Last clearing of "show interface" counters never
  Hardware is OSC_phy_port
  Internet address is 1.0.0.3/16
  MTU 1492 bytes, BW 10000000 Kbit, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     14719 packets output, 971930 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to display wdm interface information. (See Table A-15 for field descriptions.)

```
Switch# show interfaces wdm 0/0
Wdm0/0 is up, line protocol is up
 Wdm Hw capability: N/A
 Num of Wavelengths Add/Dropped: 5
 List of Wavelengths: 0, 25, 26, 27, 28
  Hardware is wavelength_add_drop
```

Table A-15 show interfaces wdm Field Descriptions

Field	Description
Wdm0/0 is up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.
Patched Interface:	Shows how the OADM modules is optically patched.
Num of wavelengths Add/Dropped:	Shows the number of wavelengths added and dropped.
List of Wavelengths:	Shows list of wavelength channel numbers.
Hardware is wavelength_add_drop	Shows the hardware type.

Related Commands

Command	Description
laser control forward enable	Configures forward laser control on transparent and wave interfaces.
laser control safety enable	Configures laser safety control on wave interfaces.

Command	Description
loopback	Configures loopback on transparent and wave interfaces.
show controllers	Displays interface controller information.

show optical filter

To display information about the channels supported by the OADM modules, use the **show optical filter** command.

show optical filter [**detail**]

Syntax Description

detail	Shows optical patch connections between the OADM modules in addition to the channels supported. This information displays only if the patch connection has been configured with the **patch** command.

Defaults

Displays only the channels supported by the OADM modules.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to verify the system configuration.

Examples

The following example shows how to display optical filter information. (See Table A-16 for field descriptions.)

```
Switch# show optical filter
aggregate                               filtered
interface            channel(s)      interface
-----------------    -----------     ------------
Wdm0/0                   0           Oscfilter0/0
Wdm0/0                   1           Filter0/0/0
Wdm0/0                   2           Filter0/0/1
Wdm0/0                   3           Filter0/0/2
Wdm0/0                   4           Filter0/0/3
Wdm0/1                   0           Oscfilter0/1
Wdm0/1                   1           Filter0/1/0
Wdm0/1                   2           Filter0/1/1
Wdm0/1                   3           Filter0/1/2
Wdm0/1                   4           Filter0/1/3
```

Table A-16 show optical filter Field Descriptions

Field	Description
aggregate interface	Shows the aggregate wdm interface.
channels	Shows the channels in the aggregate interface. In the output example, “remaining” indicates that whichever channels have not been dropped are passed to the thru interface.
filtered interface	Shows the filtered interface.
remaining	Indicates that the channels not supported on the OADM modules are passed thru to the next OADM module.
patched mux/demux interface	Shows the patch connection to another OADM module.

The following example shows how to display optical filter information on a shelf with OADM modules. (See Table A-17 for field descriptions.)

```
Swtich# show optical filter detail
aggregate                          filtered             patched mux/demux
interface           channel(s)     interface            interface
-----------------   -----------    -----------------    -----------------
Wdm0/0                  0          Oscfilter0/0
Wdm0/0                  1          Filter0/0/0
Wdm0/0                  2          Filter0/0/1
Wdm0/0                  3          Filter0/0/2
Wdm0/0                  4          Filter0/0/3
Wdm0/0              remaining      Thru0/0
Wdm0/1                  0          Oscfilter0/1
Wdm0/1                  1          Filter0/1/0
Wdm0/1                  2          Filter0/1/1
Wdm0/1                  3          Filter0/1/2
Wdm0/1                  4          Filter0/1/3
Wdm0/1              remaining      Thru0/1
```

Table A-17 show optical filter detail Field Descriptions

Field	Description
aggregate interface	Shows the aggregate wdm interface.
channels	Shows the channels in the aggregate interface. In the output example, “remaining” indicates that whichever channels have not been dropped are passed to the thru interface.
filtered interface	Shows the filtered interface.
remaining	Indicates that the channels not supported on the OADM modules are passed thru to the next OADM module.
patched mux/demux interface	Shows the patch connection to another OADM module.

Related Commands

Command	Description
patch	Configures patch connections for a shelf.

Command	Description
show connect	Displays optical connection information.
show patch	Displays optical patch connection configuration.

show patch

To display the patch connections, use the **show patch** command.

show patch [**detail**]

Syntax Description

detail	Displays both the user and automatic local path connections.

Defaults

Displays summary patch connection information.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the patch connections on the OADM modules configured with the **patch** command.

The error field in the **show patch** command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a transponder line card and an OADM module, "Channel Mismatch" appears for the patch connection. When more than one OADM module drops the same channels, "Channel Mismatch" appears for all patch connections.

Examples

The following example shows how to display patch connection information. (See Table A-18 for field descriptions.)

```
Switch# show patch
Patch Interface     Patch Interface     Type       Dir   Error
------------------  ------------------  ---------  ----  ----------------
Oscfilter0/1        Wave2/1             USER       Both
Oscfilter0/0        Wave2/0             USER       Both
Filter0/1/2         Wavepatch10/0/0     USER       Both
Filter0/0/1         Wavepatch8/0/0      USER       Both
Filter0/1/1         Wavepatch8/0/1      USER       Both
Filter0/1/3         Wavepatch4/0/0      USER       Both
Filter0/0/2         Wavepatch7/0/1      USER       Both
```

The following example shows how to display detailed patch connection information. (See Table A-18 for field descriptions.)

```
Switch# show patch detail
Patch Interface     Patch Interface     Type       Dir   Error
------------------  ------------------  ---------  ----  ----------------
Oscfilter0/1        Wave2/1             USER       Both
Oscfilter0/0        Wave2/0             USER       Both
Filter0/0/2         Wavepatch7/0/1      USER       Both
Filter0/0/1         Wavepatch8/0/0      USER       Both
Filter0/1/2         Wavepatch10/0/0     USER       Both
Filter0/1/1         Wavepatch8/0/1      USER       Both
Filter0/1/3         Wavepatch4/0/0      USER       Both

Switch# show patch detail
Patch Interface      Patch Interface      Type         Error
-----------------    -----------------    ---------    ----------------
Filter0/0/0          Wavepatch7/0/0       AUTOMATIC    Channel Mismatch
```

Table A-18 show patch detail Field Descriptions

Field	Description
Patch Interface	Shows an interface identifier for the patch connection.
Type	Shows how the patch was configured, either by the system or by the user.
Error	Shows patch errors, such as channel mismatches.

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
patch	Configures patch connections within a shelf.

shutdown

To disable an interface, use the **shutdown** command. To restart a disabled interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Usage Guidelines

This command disables all functions on the specified interface.

This command also marks the interface as unavailable. To check whether an interface is disabled, use the **show interfaces** command. An interface that has been shut down is shown as administratively down in the **show interfaces** output.

On transparent and wave interfaces, use the **shutdown** command to turn off the transmit lasers. To turn the transmit lasers on, use the **no shutdown** command.

A **shutdown** command issued on a wave, waveethernetphy, or tengigethernetphy interface does not affect administrative status of the corresponding wavepatch interfaces. To administratively shut down the wavepatch interfaces, issue **shutdown** commands directly.

To use splitter line cards for line card protection, you must shut down all the wavepatch interfaces. (See the "Examples" section.)

Examples

The following example shows how to shut down a wave interface, which also turns off the laser that transmits to the trunk fiber.

```
Switch# configure terminal
Switch(config)# interface wave 3/0
Switch(config-if)# shutdown
```

The following example shows how to reenable a transparent interface and turn on the laser transmitting to the client equipment.

```
Switch# configure terminal
Switch(config)# interface transparent 8/0/0
Switch(config-if)# no shutdown
```

The following example shows how to disable the east (slot 1) side of the wavepatch interface pair on a splitter protected line card motherboard.

```
Switch# configure terminal
Switch(config)# interface wavepatch 3/0/1
Switch(config-if)# shutdown
```

Related Commands

Command	Description
show interfaces	Displays system interfaces.

Online Diagnostics Commands

Online diagnostics test the accessibility of the components on the Cisco ONS 15530. Use the following commands to configure and monitor online diagnostic operations.

diag online

To enable online diagnostics for the system, use the **diag online** command. To disable online diagnostics for the system, use the **no** form of this command.

diag online

no diag online

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable or disable online diagnostics for the system. Online diagnostics run in background mode or during OIR (online insertion and removal). Any slot level diagnostics previously configured with the**diag online slot** command take precedence over the **diag online** command.

When online diagnostics are disabled, no further diagnostics can run.

Examples

The following example shows how to enable online diagnostics.

```
Switch# configure terminal
Switch(config)# diag online
```

Related Commands

Command	Description
debug diag online	Enables debugging of the online diagnostics.
diag online slot	Enables online diagnostics for a specified slot number.
show diag online	Displays the configuration and status of the online diagnostics.

diag online slot

To enable online diagnostics for a specified slot number, use the **diag online slot** command. To disable online diagnostics for a specific slot number, use the **no** form of this command.

diag online slot *slot-number*

no diag online slot *slot-number*

Syntax Description

slot-number	Specifies the number of the slot on which to run online diagnostics. The range is 0 to 11.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable or disable online diagnostics for a specified slot number. It can be useful to disable online diagnostics on a particular slot when there is a spurious error that causes excessive console messages.

Examples

The following example shows how to enable online diagnostics for a specific slot number.

```
Switch# configure terminal
Switch(config)# diag online slot 2
```

The following example shows how to enable online diagnostics on all the slots and then disable online diagnostics for a specific slot number.

```
Switch# configure terminal
Switch(config)# diag online
Switch(config)# no diag online slot 10
```

Related Commands

Command	Description
debug diag online	Enables debugging of the online diagnostics.
diag online	Enables online diagnostics for the system.
show diag online	Displays the configuration and status of the online diagnostics.

show diag online

To display current online diagnostic test results, use the **show diag online** command. Information displayed includes the cards installed, their current status, and the status of online tests performed on the cards.

show diag online

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command whenever a card is unavailable or is not coming up, to determine card status and the status of various background online tests performed on them.

Examples

The following example shows how to display online diagnostic test results for the hardware components. (See Table A-19 for field descriptions.)

```
Switch# show diag online
Online Diagnostics Current Summary Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    21 hours, 52 minutes

 Slot       CardType         Enabled     Bootup/    Periodic     Previous
                                        Insertion   Background   Failures
                                        tests       tests
 ~~~~~~   ~~~~~~~~~~~~~~     ~~~~~~~   ~~~~~~~~~   ~~~~~~~~~~    ~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd       Yes      Pass          Pass           No
 0/ 3/*Mx-DMx-8Mod-Plus1-W      Yes      Pass          Pass           No

 1/*/*      Mx-DMx-Mthrbd       Yes      Pass          Pass           No
 1/ 3/*Mx-DMx-8Mod-Plus1-W      Yes      Pass          Pass           No

 6/*/*         Queens CPU       Yes      Pass          Pass           No

 7/*/*         Queens CPU       Yes      Pass          Pass           No

10/*/*   XpndrMotherboard       Yes      Pass          Pass           No
10/ 0/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
10/ 1/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
10/ 2/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
10/ 3/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
```

Table A-19 show diag online Field Descriptions

Field	Description
Slot	Shows the slot on which online diagnostics have been run.
CardType	Shows the card type on which online diagnostics have been run.
Enabled	Indicates whether online diagnostic tests are enabled on the slot.
Bootup/Insertion tests	Indicates whether the card passed the test run at system bootup or when the component is inserted in the chassis.
Periodic Background tests	Indicates whether the card passed the periodic background tests.
Previous Failures	Shows when the last failure occurred for the component.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
show diag online detail	Shows detailed online diagnostic test results for the shelf.
show diag online slot	Shows detailed online diagnostic test results for a specific slot.

show diag online detail

To display the cards currently installed on the system and the detailed results of online diagnostic tests performed on them, use the **show diag online detail** command.

show diag online detail

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display detailed status information about all the online diagnostic tests run on the hardware in the system. Information displayed includes the number of times background tests passed or failed, as well as the status of OIR tests.

Use this command to debug possible hardware problems on the cards or subcards installed.

Examples

The following example shows how to display current, detailed online diagnostics for the system. (See Table A-20 for field descriptions.)

```
Switch# show diag online detail

Online Diagnostics Detailed Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    21 hours, 57 minutes

___________________________________________________________________________
Slot[0]:Mx-DMx-Mthrbd
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes       never
                          idpromAccess      Pass
 0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass    0 minutes       never

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass21 hours, 57        never
                          idpromAccess      Pass
```

```
 0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass21 hours, 57        never
___________________________________________________________________________
Slot[1]:Mx-DMx-Mthrbd
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 1/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes       never
                          idpromAccess      Pass
 1/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass    0 minutes       never

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 1/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass21 hours, 57        never
                          idpromAccess      Pass
 1/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass21 hours, 57        never
___________________________________________________________________________
Slot[6]:Queens CPU
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 6/*/*         Queens CPU    srcStatus      Pass    0 minutes       never
                             PCIAccess      Pass
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
                          PCMCIAAccess      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 6/*/*         Queens CPU    srcStatus      Pass21 hours, 57        never
                             PCIAccess      Pass
                          PCMCIAAccess      Pass
___________________________________________________________________________
Slot[7]:Queens CPU
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 7/*/*         Queens CPU    srcStatus      Pass    0 minutes       never
                             PCIAccess      Pass
                          PCMCIAAccess      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 7/*/*         Queens CPU    srcStatus      Pass21 hours, 51        never
                             PCIAccess      Pass
                          PCMCIAAccess      Pass
___________________________________________________________________________
Slot[10]:XpndrMotherboard
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/*/*   XpndrMotherboard    lrcAccess      Pass    0 minutes       never
                          idpromAccess      Pass
10/ 0/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
```

```
                           idpromAcces      Pass
10/ 1/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass
10/ 2/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass
10/ 3/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/*/*   XpndrMotherboard    lrcAccess      Pass21 hours, 57        never
                          idpromAccess      Pass
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/ 0/*  NPlugXpndrMonitor    scAccess      Pass21 hours, 57        never
                           idpromAcces      Pass
10/ 1/*  NPlugXpndrMonitor    scAccess      Pass21 hours, 57        never
                           idpromAcces      Pass
10/ 2/*  NPlugXpndrMonitor    scAccess      Pass21 hours, 57        never
                           idpromAcces      Pass
10/ 3/*  NPlugXpndrMonitor    scAccess      Pass21 hours, 57        never
                           idpromAcces      Pass
```

Table A-20 show diag online detail Field Descriptions

Field	Description
On ACTIVE CPU card Slot:	Shows the chassis slot that contains the active CPU switch module.
CPU Uptime	Shows the amount of time since the system booted.
Slot	Shows the slot on which the online diagnostics are being run.
Enabled	Indicates whether online diagnostics are enabled on the slot.
CardType	Shows the card type on which the online diagnostics are being run.
TestType	Shows the type of test run. Test types can be: • lrcAccess (Accesses the LRC) • idpromAccess (Accesses the IDPROM) • srcAccess (Accesses the SRC) • PCMCIAAccess (Accesses Flash PC Cards • scAccess (Accesses transponder line cards)
Status	Shows the result of the diagnostic test (Pass/Fail)
LastRunTime	Shows the amount of time since the test was last run.
LastFailTime	Shows the amount of time since the test failed.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
show diag online	Shows a summary of the online diagnostic test results for the shelf.
show diag online slot	Shows detailed online diagnostic test results for a specific slot.

show diag online slot

To display the results of online diagnostic tests performed on a card in a specific slot, use the **show diag online slot** command.

show diag online slot *slot-number*

Syntax Description

slot-number	Specifies the slot number. The range is 0 to 11.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the status of online diagnostics performed on components installed in a specific slot.

Examples

The following example shows how to display the results of online diagnostic tests performed on slot 0. (See Table A-21 for field descriptions.)

```
Switch# show diag online slot 0
Online Diagnostics Information Per Slot
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Slot[0]:Mx-DMx-Mthrbd
Enabled: Yes
CPU Uptime:    21 hours, 59 minutes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes       never
                          idpromAccess      Pass
 0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass    0 minutes       never

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass21 hours, 58        never
                          idpromAccess      Pass
 0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces      Pass21 hours, 58        never
```

Table A-21 show diag online slot Field Descriptions

Field	Description
Slot	Shows the slot on which online diagnostics were performed.
Enabled	Indicates whether online diagnostics are enabled on the slot.
CPU Uptime	Shows the amount of time since the system booted.
CardType	Shows the card type on which the online diagnostics are being run.
TestType	Shows the type of test run. Test types can be: • lrcAccess (accesses the LRC) • idpromAccess (accesses the IDPROM) • srcAccess (accesses the SRC) • PCMCIAAccess (accesses Flash PC Cards) • scAccess (accesses transponder line cards)
Status	Shows the result of the diagnostic test (Pass/Fail).
LastRunTime	Shows the amount of time since the test was last run.
LastFailTime	Shows the amount of time since the test failed.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
show diag online	Shows a summary of the online diagnostic test results for the shelf.
show diag online detail	Shows detailed online diagnostic test results for the shelf.

OSCP Commands

OSCP (Optical Supervisory Channel Protocol) provides out-of-band network management over a 33rd channel. Use the following commands to configure and monitor OSCP operations.

clear oscp

To clear OSCP statistics or traffic counters, use the **clear oscp** command.

clear oscp {**statistics** | **traffic**}

Syntax Description

statistics	Clears OSCP statistics that can be used to debug the protocol, for example: • The hold-down count statistic specifies how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets. • The Hello Tx and Rx statistics indicate the number of Hello packets that have been transmitted and received at an interface. • The OSCP go-down statistic indicates the number of times an interface has gone out of the two-way state.
traffic	Clears OSCP control-traffic counters that indicate the number of different protocol packets that were transmitted over the optical supervisory channel.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to perform a one-time clear of the specified OSCP statistics or traffic tables. This command is useful for debugging or monitoring OSCP performance.

Examples

The following example shows how to clear OSCP statistics and traffic tables.

```
Switch# clear oscp statistics
Switch# clear oscp traffic
```

Related Commands

Command	Description
show oscp statistics	Displays OSCP Hello statistics information.
show oscp traffic	Display OSCP Hello traffic information.

oscp timer hello holddown

To modify the OSCP timer Hello hold-down interval, use the **oscp timer hello holddown** command. To return the Hello hold-down interval to its default value, use the **no** form of the command.

oscp timer hello holddown *milliseconds*

no oscp timer hello holddown

Syntax Description

milliseconds	Specifies, in milliseconds, the interval in which no more than one Hello packet can be generated. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. The range is 150 to 30000 milliseconds.

Defaults

3000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to control the amount of OSCP Hello activity that is generated on the network. The Hello hold-down timer specifies the interval during which no more than one Hello packet can be sent. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. Increasing the hold-down timer limits the number of Hello packets triggered in response to Hello packets received from a neighboring node and reduces the likelihood of Hello packets flooding the OSC.

To ensure proper functioning of the OSCP, the Hello hold-down timer value can be no more that 75 percent of the OSCP Hello interface timer.

Note There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples

The following example shows how to configure the OSCP timer Hello hold-down interval.

```
Switch# configure terminal
Switch(config)# oscp timer hello holddown 300
```

Related Commands

Command	Description
debug driver voa	Enables debugging of OSCP activity.
oscp timer hello interval	Modifies the OSCP timer Hello interval.
oscp timer inactivity-factor	Modifies the OSCP timer inactivity factor.
show oscp info	Displays OSCP configuration information.

oscp timer hello interval

To modify the OSCP timer Hello interval, use the **oscp timer hello interval** command. To return the Hello interval to its default value, use the **no** form of the command.

oscp timer hello interval *milliseconds*

no oscp timer hello interval

Syntax Description

milliseconds	Specifies, in milliseconds, the periodic generation of OSCP Hello packets. The range is 100 to 10000 milliseconds.

Defaults

100 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to control how often OSCP Hello messages are sent. The OSCP sends Hello packets to adjacent nodes at a configured interval. When five packets fail to get a response from the receiving node, that node is declared "down." By decreasing the interval at which Hello packets are sent, reaction time to a failed node can be lessened. Increasing the interval reduces the amount of Hello packet traffic.

Note There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples

The following example shows how to configure the OSCP timer Hello interval.

```
Switch# configure terminal
Switch(config)# oscp timer hello interval 200
```

Related Commands

Command	Description
debug driver voa	Enables debugging of OSCP activity.
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer inactivity-factor	Modifies the OSCP timer Hello inactivity factor.
show oscp info	Displays OSCP configuration information.

oscp timer inactivity-factor

To modify the OSCP timer Hello inactivity factor, use the **oscp timer inactivity-factor** command. To return the Hello inactivity factor to its default value, use the **no** form of the command.

oscp timer inactivity-factor *factor*

no oscp timer inactivity-factor

Syntax Description

factor	Specifies a value used to calculate an inactivity interval. The specified interval of time is equal to the inactivity factor multiplied by the neighbor's advertised Hello interval. The range is 1 to 50.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The system uses this attribute to determine when a neighbor node, or the link to it, has gone down. The link to a neighbor node is considered inactive if an OSCP Hello packet is not received for a time interval determined by the inactivity factor. The time interval is calculated by multiplying the inactivity factor by the advertised hold-down interval. For example, if the neighbor node's advertised hold-down interval is 5 seconds and the local node's inactivity factor is 5, the time interval that the local node will wait until declaring the neighbor node down is 25 seconds.

Note There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples

The following example shows how to set the OSCP timer Hello inactivity factor to 3.

```
Switch# configure terminal
Switch(config)# oscp timer inactivity-interval 3
```

Related Commands

Command	Description
debug driver voa	Enables debugging of OSCP activity.
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.

Command	Description
oscp timer hello interval	Modifies the OSCP timer Hello interval.
show oscp info	Displays OSCP configuration information.

show oscp info

To display OSCP (Optical Supervisory Channel Protocol) configuration information, use the **show oscp info** command.

show oscp info

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display OSCP configuration information for the system.

Examples

The following example shows how to display OSCP configuration information for the system. (See Table A-22 for field descriptions.)

```
Switch# show oscp info
OSCP protocol version 1, Node ID        0000.1644.28fb
No. of interfaces 1, No. of neighbors 1
Hello interval 50 tenth of sec, inactivity factor 5,

Hello hold-down 1 tenth of sec
Supported OSCP versions: newest 1, oldest 1
```

Table A-22 show oscp info Field Descriptions

Field	Description
OSCP protocol version	Shows the OSCP version.
Node ID	Shows the node ID.
No. of interfaces	Shows the number of interfaces.
No. of neighbors	Shows the number of neighbors.
Hello interval	Shows the Hello interval in milliseconds.

Table A-22 show oscp info Field Descriptions (continued)

Field	Description
inactivity factor	Shows the inactivity factor. The system uses the inactivity factor to determine when a link has gone down. A link is returned to the "attempt" state if the system has not received an OSCP Hello packet for a certain time interval. That time interval is equal to the Hello inactivity factor multiplied by the Hello interval from the Hello packet most recently received from the remote system. The range of inactivity factors is from 2 to 50. The default inactivity factor is 5.
Hello hold-down	Shows, in milliseconds, how long to wait before sending another OSCP Hello packet. This avoids excessive generation of OSCP Hello packets.
Supported OSCP versions	Shows the OSCP versions supported.

Related Commands

Command	Description
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer hello interval	Modifies the OSCP timer Hello interval.
oscp timer inactivity-factor	Modifies the OSCP timer inactivity factor.

show oscp interface

To display OSCP (Optical Supervisory Channel Protocol) status information for the OSC interfaces, use the **show oscp interface** command.

show oscp interface [**wave** *slot*/*subcard*]

Syntax Description

wave *slot*	Specifies an OSC wave interface.

Defaults

Displays OSCP status information for all OSC wave interfaces in the system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display status information for the local and remote interfaces running OSCP.

Examples

The following example shows how to display status information for the local and remote interfaces running OSCP. (See Table A-23 for field descriptions.)

```
Switch# show oscp interface wave 3/0
Codes: Bndl - bundling identifier, Pri - OSCP selection priority
       OSCP - dedicated wavelength channel, CDL - in-band wavelength channel

OSCP Interface(s)
 Local Port    Port ID Type Status  OSCP St Bndl Pri  Rem Port ID Rem Node Id
 ~~~~~~~~~~~~~ ~~~~~~~ ~~~~ ~~~~~~  ~~~~~~~ ~~~~ ~~~  ~~~~~~~~~~~ ~~~~~~~~~~~~~~
  Wave3/0         1000000 OSCP  Active  2way      0   0  1000000     0000.1644.28fb
```

Table A-23 show oscp interface Field Descriptions

Field	Description
Local Port	Shows the local port for the OSCP interface.
Port ID	Shows the port ID for the local port.
Type	Shows the channel link type, either OSCP or in-band message channel.
Status	Shows the local port status (active or standby).

Table A-23 show oscp interface Field Descriptions (continued)

Field	Description
OSCP St	Shows the OSCP Hello state. Valid values are: • down—the physical layer is down • attempt—the physical layer is up, but no Hello messages have been received from the neighbor • 1-way—Hello messages have been received from the neighbor, but their content indicates that the neighbor has not yet received Hellos from this node. • 2-way—Hello messages have been received from the neighbor indicating that the neighbor has received Hello packets from this node.
Bndl	Shows the bundling identifier, which identifies the wavelength bundle to the remote node for the link. The bundle identifier is carried in the OSCP Hello packet. The configured bundle identifier is used to derive an identifier that both the host and remote nodes agree on. By default, all links have a zero (0) value. Because all links have the same default value, all links between the host and remote nodes are aggregated into a single logical link (with bundle identifier 0). To assign a non-default bundle identifier to a link between two nodes, only one side has to be configured with the non-default value. The default value 0 indicates that the host node uses the bundle identifier on the remote node. Valid values are 0-255. **Note** The bundling identifier is supported in this release.
Pri	Shows OSC selection priority. When multiple links are present in the same wavelength bundle, the link with the highest priority value is selected as the active OSC link. The OSC link transmits all control and network management traffic for the entire wavelength bundle to the remote node. Only links that have a LinkHelloState value of "two-way" can be the active OSC link. If more than one link has the highest link priority, the selection is arbitrary. To ensure that a specific link is chosen to be the active OSC link, its priority value must be higher than all other links. Valid priority values are 0-255. **Note** The OSC selection priority is supported in this release.
Rem Port ID	Shows the port ID for the remote port.
Rem Node Id	Shows the node ID for the remote port.

Related Commands

Command	Description
show oscp neighbor	Displays OSCP neighbor information.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.

show oscp neighbor

To display OSCP (Optical Supervisory Channel Protocol) neighbor information, use the **show oscp neighbor** command.

show oscp neighbor

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display information about the identity of the neighbors communicating with the system through OSCP.

Examples

The following example shows how to display information about the identity of the neighbors communicating with the system through OSCP. (See Table A-24 for field descriptions.)

```
Switch# show oscp neighbor
OSCP Neighbors
   Neighbor Node Id: 0000.1644.28ff   Port list:
    Local Port    Port ID  Rem Port ID OSCP state
   ~~~~~~~~~~~~~ ~~~~~~~~ ~~~~~~~~~~~ ~~~~~~~~~
   Wave3/0         1000000   1000000     2way
```

Table A-24 show oscp neighbor Field Descriptions

Field	Description
Neighbor Node Id	Shows the node ID for the OSCP neighbor.
Port list	Shows ports and port IDs for local and remote ports.
Local Port	Shows the local port.
Port Id	Shows the port ID of the local port.

Table A-24 show oscp neighbor Field Descriptions (continued)

Field	Description
Rem Port ID	Shows the port ID of the remote port.
OSCP St	Shows the OSCP Hello state. Valid values are: • down—the physical layer is down • attempt—the physical layer is up, but no Hello messages have been received from the neighbor • 1-way—Hello messages have been received from the neighbor, but their content indicates that the neighbor has not yet received Hellos from this node. • 2-way—Hello messages have been received from the neighbor indicating that the neighbor has received Hello packets from this node.

Related Commands

Command	Description
show oscp interface	Displays OSCP information for an interface.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.

show oscp statistics

To display OSCP (Optical Supervisory Channel Protocol) Hello statistics, use the **show oscp statistics** command.

show oscp statistics [**wave** *slot*/*subcard*]

Syntax Description

wave *slot*	Specifies an OSC wave interface.

Defaults

Displays OSCP statistics for all OSC wave interfaces in the system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display OSCP Hello statistics for an OSC interface.

This command displays the following OSCP statistics, which can be used to debug the OSCP.

- hold down—Shows how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets.
- Hello Tx pkts and Hello Rx pkts—Shows the number of OSCP Hello packets that have been transmitted and received at an interface.
- OSCP go down—Shows the number of times an OSC interface has gone out of two-way state.

Examples

The following example shows how to display OSCP control statistics for an OSC interface. (See Table A-25 for field descriptions.)

```
Switch# show oscp statistics wave 3/0
OSCP Hello Statistics:

interface Wave3/0
 Event                   Count
~~~~~~~~~~~~             ~~~~~~~~~~
hold down                3
Hello Tx pkts            2262
Hello Rx pkts            2259
Hello discards in        0
Hello discards out       0
OSCP go down events      2

 Event                   Time (seconds)
~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~
Next Tx Hello due        2
Last Hello sent          2
Last Hello received      4
Inactivity interval      25.0
Time until port dropped 20
```

Table A-25 show oscp statistics Field Descriptions

Field	Description
hold down	Shows how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets.
Hello Tx pkts	Shows the number of Hello transmissions that have been sent.
Hello Rx pkts	Shows the number of Hello transmissions that have been received.
Hello discards in	Shows the number of incoming Hello transmissions that have been discarded.
Hello discards out	Shows the number of outgoing Hello transmissions that have been discarded.
OSCP go down events	Shows the number of times that the OSCP (Optical Supervisory Channel Protocol) has gone down.
Next Tx Hello due	Shows the number of seconds before the next transmit Hello packet is due.
Last Hello sent	Shows the number of seconds since a Hello packet was sent.
Last Hello received	Shows the number of seconds since a Hello packet was received.
Inactivity interval	Shows the number of seconds for the inactivity interval.
Time until port dropped	Shows the number of seconds allowed until the port is dropped.

Related Commands

Command	Description
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer hello interval	Modifies the OSCP timer Hello interval.

show oscp traffic

To display OSCP (Optical Supervisory Channel Protocol) Hello message traffic information, use the **show oscp traffic** command.

show oscp traffic [**wave** *slot*/*subcard*]

Syntax Description

wave *slot*	Specifies an OSC wave interface.

Defaults

Displays OSCP Hello message traffic information for all OSC wave interfaces in the system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display OSCP control traffic statistics, which show the count of different protocol packets that have been transmitted over the optical supervisory channel.

Examples

The following example shows how to display OSCP control traffic statistics, which show the count of different protocol packets that have been transmitted over the optical supervisory channel. (See Table A-26 for field descriptions.)

```
Switch# show oscp traffic wave 3/0
OSC Traffic Statistics:

interface Wave3/0
Description         Count
~~~~~~~~~~~~        ~~~~~~~~~~
Tx IP pkt           0
Rx IP pkt           0
Tx CDP pkt          198
Rx CDP pkt          195
Rx pkt dropped      0
```

Table A-26 show oscp traffic Field Descriptions

Field	Description
Tx IP pkt	Shows number of IP packets that have been transmitted over the optical supervisory channel.
Rx IP pkt	Shows number of IP packets that have been received over the optical supervisory channel.

Table A-26 show oscp traffic Field Descriptions (continued)

Field	Description
Tx CDP pkt	Shows number of CDP packets that have been transmitted over the optical supervisory channel.
Rx CDP pkt	Shows number of CDP packets that have been received over the optical supervisory channel.
Rx pkt dropped	Shows the number of receive packets that were dropped.

Related Commands

Command	Description
clear oscp	Clears OSCP statistics or traffic counters.

CPU Switch Module Redundancy Commands

CPU switch module redundancy provides protection against CPU switch module failure. Use the following commands to configure and monitor CPU switch module redundancy operations.

auto-sync running-config

To selectively enable only automatic synchronizing of the running configuration on the active processor to the standby CPU switch module, use the **auto-sync running-config** command. To disable automatic synchronizing of the running configuration, use the **no** form of this command.

auto-sync running-config

no auto-sync running-config

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable or disable automatic synchronizing of the running configuration without affecting the following types of synchronization:

- Startup configuration
- Dynamic database synchronizing

When a CPU switch module switchover occurs, the standby CPU switch module normally uses the running configuration rather than the startup configuration. However, if **auto-sync running-config** is disabled when a CPU switch module switchover occurs, the standby CPU switch module uses the startup configuration.

In maintenance mode, all database synchronizing to the standby CPU switch module is disabled even if **auto-sync running-config** is enabled.

Examples

The following example shows how to disable automatic synchronizing of the running configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# no auto-sync running-config
```

Related Commands

Command	Description
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby CPU switch module.
maintenance-mode	Disables all CPU switch module redundancy synchronization.
redundancy	Enters redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time database update.
show bootvar	Displays boot and other environmental variables.
show redundancy	Displays CPU switch module redundancy status and configuration information.

auto-sync startup-config

To selectively enable only automatic synchronizing of the startup configuration to the standby CPU switch module, use the **auto-sync startup-config** command. To disable automatic synchronizing of the startup configuration, use the **no** form of this command.

auto-sync startup-config

no auto-sync startup-config

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable or disable only automatic synchronizing of the startup configuration without affecting the following synchronization:

- Running configuration
- Dynamic database synchronizing

In maintenance mode, all database synchronizing to the standby CPU switch module is disabled even if **auto-sync startup-config** is enabled.

Examples

The following example shows how to disable automatic synchronizing of the startup configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# no auto-sync startup-config
```

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby CPU switch module.
maintenance-mode	Disables all CPU switch module redundancy synchronization.
redundancy	Enters redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time database update.

Command	Description
show bootvar	Displays boot and other environmental variables.
show redundancy	Displays CPU switch module redundancy status and configuration information.

clear redundancy

To clear redundancy history or counters, use the **clear redundancy** command.

clear redundancy {**history** | **counters**}

Syntax Description

history	Clears the redundancy event history log.
counters	Clears the redundancy internal operational counters.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to perform a one-time clear of the specified redundancy history or statistics database. This command may be useful for debugging or monitoring redundancy performance.

Examples

The following example shows how to clear the redundancy history log.

```
Switch# clear redundancy history
```

Related Commands

Command	Description
show redundancy counters	Displays redundancy software counter information.
show redundancy history	Displays redundancy software history information.

maintenance-mode

To disable all CPU switch module redundancy synchronization, use the **maintenance-mode** redundancy command. To reenable redundancy synchronization, use the **no** form of this command.

maintenance-mode

no maintenance-mode

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

In maintenance mode, the active CPU switch module does not automatically synchronize information to the standby CPU switch module. No standby CPU switch module errors and alarms are reported to the active CPU switch module. The standby CPU switch module leaves the hot-standby mode, enters the negotiation state, and transitions to the cold-standby state.

When maintenance mode is disabled, the standby CPU switch module reloads until it reaches the hot-standby state.

Maintenance mode is useful for CPU switch module maintenance operations and system image troubleshooting.

Note We do not recommend leaving the active and standby CPU switch modules in maintenance mode for extended periods because any added configuration is lost unless the startup configuration on the active CPU switch module is manually updated and manually synchronized with the standby CPU switch module.

Examples

The following example shows how to enable maintenance mode redundancy.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# maintenance-mode
This command will place the system in SIMPLEX mode [confirm] y
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
show redundancy	Displays CPU switch module redundancy status and configuration information.

redundancy

To switch to redundancy configuration mode, use the **redundancy** command.

redundancy

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to gain access to both CPU switch module redundancy configuration commands and APS configuration commands.

Examples

The following example shows how to switch to redundancy configuration mode.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)#
```

Related Commands

Command	Description
associate group	Associates wavepatch interfaces for APS splitter protection.
associate interface	Associates two interfaces for APS protection.
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby CPU switch module.
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby CPU switch module.
maintenance-mode	Enables or disables CPU switch module redundancy synchronization.

redundancy manual-sync

To cause an immediate one-time database update of the specified database information, use the **redundancy manual-sync** command.

redundancy manual-sync {**running-config** | **startup-config** | **both**}

Syntax Description

running-config	Causes an immediate one-time update of the running configuration to the standby CPU switch module.
startup-config	Causes an immediate one-time update of the startup configuration to the standby CPU switch module.
both	Causes an immediate one-time update of the running configuration and the startup configuration to the standby CPU switch module.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command is not usually required because automatic synchronization is enabled by default and, upon exiting global configuration mode, the running configuration is updated on the standby CPU switch module. (Exit global configuration mode by entering **Ctrl-Z** or **end**.) The startup configuration is updated when the **copy** command is issued.

If auto-synchronizing is disabled, the **redundancy manual-sync** command updates the standby processor database information to be identical with the active CPU switch module.

If the system is unable to complete the update, an error message is displayed.

This command is only allowed on the active CPU switch module.

Examples

The following example shows how to make the active CPU switch module send an update for both the running configuration and the startup configuration to the standby CPU switch module.

```
Switch# redundancy manual-sync both
```

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby CPU switch module.
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

redundancy reload peer

To reload the standby CPU switch module, use the **redundancy reload peer** command.

redundancy reload peer

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to reload the standby (or peer) CPU switch module.

The active CPU switch module is allowed to reload a standby CPU switch module that is fully running the Cisco IOS software by using an NMI (non-maskable interrupt).

This command will not succeed on the active CPU switch module if the standby CPU switch module has not fully loaded its system IOS image and reached the hot-standby state.

This command cannot be entered on the standby CPU switch module.

Examples

The following example shows how to reload the standby CPU switch module.

```
Switch# redundancy reload peer
Reload peer [confirm] y
Preparing to reload peer
```

Related Commands

Command	Description
maintenance-mode	Enables or disables CPU switch module redundancy synchronization.
redundancy reload shelf	Reloads both CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the standby CPU switch module.
reload	Reloads the active CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

redundancy reload shelf

To reload both redundant CPU switch modules, use the **redundancy reload shelf** command.

redundancy reload shelf

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command causes both CPU switch modules to reload.

Examples

The following example shows how to reload the entire shelf.

```
Switch# redundancy reload shelf
Reload the entire shelf [confirm] y
Preparing to reload shelf
```

Related Commands

Command	Description
maintenance-mode	Enables or disables CPU switch module redundancy synchronization.
redundancy reload peer	Reloads the standby CPU switch module.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the standby CPU switch module.
reload	Reloads the active CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

redundancy switch-activity

To manually switch activity from the active CPU switch module to the standby CPU switch module, use the **redundancy switch-activity** command.

redundancy switch-activity [**force**]

Syntax Description

force	Forces a switch of activity even when the standby CPU switch module has not reached the hot-standby state, or if some other software condition is preventing a normal switchover from occurring.

Defaults

The active CPU switch module switches over only if the standby CPU switch module has reached hot-standby mode.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command must be issued on the active CPU switch module. It takes effect if the CPU switch module is in a state to allow switchover; that is, the standby CPU switch module is in the “Standby Hot” state and platform software is not temporarily disallowing the switchover.

Examples

The following example shows how to switch activity to the standby CPU switch module.

```
Switch# redundancy switch-activity
Preparing to switch activity
This will reload the active unit and force a switch of activity [confirm] y

01:40:35: %SYS-5-RELOAD: Reload requested
```

Related Commands

Command	Description
maintenance-mode	Enables or disables CPU switch module redundancy synchronization.
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both CPU switch modules in the shelf.
reload	Reloads the active CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy

To display a summary of active and standby CPU switch module redundancy information, use the **show redundancy** command.

show redundancy

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display a summary of redundancy-related information, including active and standby slots, uptimes, images, and current alarms. This information is useful for troubleshooting CPU switch module redundancy problems.

Examples

The following example shows how to display a summary of redundancy-related information for the system. (See Table A-27 for field descriptions.)

```
Switch# show redundancy


Redundant system information
----------------------------
Available Uptime:              12 minutes
Time since last switchover:    6 minutes
Switchover Count:              2

Inter-CPU Communication State:UP
Last Restart Reason:           Switch over
Reported Switchover Reason:    User initiated
Software state at switchover:  STANDBY HOT

Last Running Config sync:      2 minutes
Running Config sync status:    In Sync
Last Startup Config sync:      2 minutes
Startup Config sync status:    In Sync

This CPU is the Active CPU.
-------------------------------
Slot:                          6
Time since CPU Initialized:    8 minutes
Image Version:                 ONS-15530 Software (ONS15530-I-M), Experimental Version
12.1(20010824:021324) [ffrazer-lh2 106]
Image File:                    tftp://171.69.1.129/ffrazer/ons15530-i-mz
Software Redundancy State:     ACTIVE
Hardware State:                ACTIVE
Hardware Severity:             0

Peer CPU is the Standby CPU.
-------------------------------
Slot:                          7
Time since CPU Initialized:    2 minutes
Image Version:                 ONS-15530 Software (ONS15530-I-M), Experimental Version
12.1(20010824:021324) [ffrazer-lh2 106]
Image File (on sby-CPU):       tftp://171.69.1.129/ffrazer/ons15530-i-mz
Software Redundancy State:     STANDBY HOT
Hardware State:                STANDBY
Hardware Severity:             0
```

Table A-27 show redundancy Field Descriptions

Field	Description
Available Uptime	Shows the elapsed time since the system began providing uninterrupted operation, including the time when either CPU switch module is active.
Time since last switchover	Shows the amount of time since the last switchover.
Switchover Count	Shows the number of times switchover has occurred during the Available Uptime.
Inter-CPU Communication State	Shows the status of IPC (interprocess communications).
Last Restart Reason	Shows the reason for the last restart. Valid reasons include normal boot and switchover.

Table A-27 show redundancy Field Descriptions (continued)

Field	Description
Last Switchover Reason	Shows the reason for the last switchover when the Last Restart Reason field shows "Switch over." Valid reasons are: • Not known • User initiated • User forced • User forced (reload) • Active unit failed • Active unit removed
Software state at switchover	Shows the software redundancy state of the processor at the time of the last switchover.
Last Running Config sync	Shows the amount of time since the CPU switch module was synchronized with the last running configuration.
Running Config sync status	Indicates whether the CPU switch module is in sync with the running configuration.
Last Startup Config sync	Shows the amount of time since the CPU switch module was synchronized with the last startup configuration.
Startup Config sync status	Indicates whether the CPU switch module is in sync with the startup configuration.
Slot	Shows the slot number on the active or standby system.
Time since CPU Initialized	Shows the amount of time since the active or standby CPU switch module was last initialized.
Image	Shows the active or standby CPU switch module system image and version.
Software Redundancy State	Indicates whether software redundancy is enabled for the active and standby CPU switch module.
Hardware State	Shows the hardware state of the active or standby CPU switch module.
Hardware Severity	Shows the severity of hardware faults. Valid values are: • 0 = good CPU switch module hardware (no hardware faults) • 1 = CPU switch module hardware fault that does not affect traffic • 2 = fault that partially affects traffic • 3 = fault that may affect all user data traffic

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.

Command	Description
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy capability	Displays CPU switch module redundancy capability information.

show redundancy capability

To display capabilities of the active and standby CPU switch modules, use the **show redundancy capability** command.

show redundancy capability

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display hardware and functional versions of the various components. If the capabilities do not match, the system is running in a degraded redundancy mode.

Examples

The following example shows how to display capabilities for the active and standby CPU switch modules. (See Table A-28 for field descriptions.)

```
Switch# show redundancy capability

CPU capability support

 Active CPU  Sby CPU    Sby Compat        CPU capability description
 ---------- ---------- ----------- ----------------------------------------
    96 MB      96 MB   OK          CPU DRAM size
    32 MB      32 MB   OK          CPU PMEM size
   512 KB     512 KB   OK          CPU NVRAM size
    16 MB      16 MB   OK          CPU Bootflash size
    3.5        3.5     OK          CPU hardware major.minor version
    1.20       1.18    OK          CPU functional major.minor version

Linecard driver major.minor versions, (counts: Active=18, Standby=18)

 Active CPU  Sby CPU   Sby Compat  Drv ID     Driver description
 ---------- ---------- ----------- ------ -----------------------------------
    1.1        1.1     OK          0x1000 CPU w/o Switch Fabric
    1.1        1.1     OK          0x1001 Fixed Transponder, w/monitor
    1.1        1.1     OK          0x1002 Fixed Transponder, no monitor
    1.1        1.1     OK          0x1003 Pluggable Transponder, w/monitor
    1.1        1.1     OK          0x1004 Pluggable Transponder, no monitor
    1.1        1.1     OK          0x1005 Line Card Motherboard
    1.1        1.1     OK          0x1006 Backplane
    1.1        1.1     OK          0x1007 32-ch Mux/Demux
    1.1        1.1     OK          0x1008 Fixed 4-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x1009 Fixed 8-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100A Modular 4-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100B Modular 8-ch Mux/Demux, no OSC
    1.1        1.1     OK          0x100C 32-ch Array Wave Guide
    1.1        1.1     OK          0x100D Mux/Demux Motherboard
    1.1        1.1     OK          0x100E Modular 4-ch Mux/Demux plus OSC
    1.1        1.1     OK          0x100F Modular 8-ch Mux/Demux plus OSC
    1.1        1.1     OK          0x1010 Mux-Demux Motherboard, no OSC
    1.1        1.1     OK          0x1011 Line Card Motherboard, no splitter

Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts: Active=2, Standby=2

 Active CPU  Sby CPU   Sby Compat  Cl ID  Redundancy Client description
 ---------- ---------- ----------- ----- -----------------------------------
 ver  1-1   ver  1-1   OK          17    CPU Redundancy
 ver  1-1   ver  1-1   OK          6     OIR Client


Backplane IDPROM comparison
 Backplane IDPROM field      Match Local CPU            Peer CPU
 --------------------------  ----- -------------------- --------------------
 idversion                   YES   1                    1
 magic                       YES   153                  153
 card_type                   YES   4102                 4102
 order_part_num_str          YES   N/A                  N/A
 description_str             YES   Manhattan_Backplane_PHASE_0
                                                        Manhattan_Backplane_PHASE_0
 board_part_num_str          YES   73-5655-03           73-5655-03
 board_revision_str          YES   02                   02
 serial_number_str           YES   TBC05031572          TBC05031572
 date_of_manufacture_str     YES   02/16/2001           02/16/2001
 deviation_numbers_str       YES   0                    0
 manufacturing_use           YES   0                    0
 rma_number_str              YES   0x00                 0x00
 rma_failure_code_str        YES   0x00                 0x00
 oem_str                     YES   Cisco_Systems        Cisco_Systems
 clei_str                    YES
 snmp_oid_substr             NO    0
 schematic_num_str           YES   92-4113-03           92-4113-03
 hardware_major_version      YES   3                    3
 hardware_minor_version      YES   0                    0
 engineering_use_str         YES   1                    1
 crc16                       OK    5913                 24184
 user_track_string           NO    lab
 diagst                      YES   ^A                    ^A
 board_specific_revision     YES   1                    1
 board_specific_magic_number YES   153                  153
 board_specific_length       YES   56                   56
 mac_address_block_size      YES   16                   16
 mac_address_base_str        YES   0000164428fb0        0000164428fb0
 cpu_number                  OK    1                    1
 optical_backplane_type      YES   255                  255
```

Table A-28 show redundancy capability Field Descriptions

Field	Description
Active CPU	Shows the following information for the active CPU switch module: • processor DRAM size—the size of dynamic random access memory • processor PMEM size—the amount of dynamic RAM reserved for packet I/O usage • processor NVRAM size—the size of nonvolatile RAM • processor Bootflash size—the size of bootflash memory • processor hardware major.minor version—the CPU switch module hardware version • processor functional major.minor version—the CPU switch module functional version
Sby CPU	Shows information for the standby CPU switch module. See the "Active CPU" description above.
Sby Compat	Indicates whether the standby CPU switch module is compatible with the active CPU switch module.
CPU capability description	Shows the capability descriptions for the active and standby CPU switch modules. See the "Active CPU" description above.
Linecard driver major.minor versions	Shows the number of line card drivers.
Drv ID	Shows the driver ID.
Driver description	Shows the driver description.
Software sync client versions	Shows the redundancy client version in the range X-Y, where: • X indicates the oldest peer version it can communicate with. • Y indicates the current sync client version. Also shows the sync client counts.
Cl ID	Shows the client ID.
Redundancy Client description	Shows the redundancy client descriptions.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy clients

To display a list of internal redundancy clients, use the **show redundancy clients** command.

show redundancy clients

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display information about the software subsystems that are clients of the platform-independent RF (Redundancy Facility) subsystem. Subsystems that need to synchronize information from the active CPU switch module to the standby CPU switch module (or vice versa) are registered as clients of the RF.

This client information can be used to debug redundancy software.

Examples

The following example shows how to display a list of internal redundancy clients. (See Table A-29 for field descriptions.)

```
Switch# show redundancy clients
 clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 6      clientSeq = 16       OIR Client
 clientID = 17     clientSeq = 40       CPU Redundancy
 clientID = 19     clientSeq = 9999     RF_LAST_CLIENT
```

Table A-29 show redundancy clients Field Descriptions

Field	Description
clientID	Shows the ID of the redundant client.
clientSeq	Shows the client notification sequence number. Client sequence numbers determine the order in which a client is notified of RF events, relative to other clients. There are cases where one client must be notified before another. This should be noted when the sequence number is defined. The lower sequence numbers are notified first.
RF_INTERNAL_MSG	Shows the RF first client, which is part of the RF subsystem and is necessary for its operation.

Table A-29 show redundancy clients Field Descriptions (continued)

Field	Description
OIR Client	Shows the OIR (online insertion and removal) client, which updates the standby CPU switch module when line cards are inserted and removed.
CPU Redundancy	Shows the CPU switch module redundancy client, which sends running or startup configuration changes to the standby CPU switch module. This client also reports hardware/software compatibility and version numbers between the CPU switch modules. It also ensures that CPU switch module arbitration changes and peer CPU switch module communication losses are reported to the RF and to other subsystems.
RF_LAST_CLIENT	Shows the RF last client, which is part of the RF subsystem and is necessary for its operation.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy counters

To display internal redundancy software counters, use the **show redundancy counters** command.

show redundancy counters

Syntax Description

This command has no other arguments or keywords

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display internal redundancy software counter information, which can be used to debug redundancy software.

Examples

The following example shows how to display internal redundancy software counter information. (See Table A-30 for field descriptions.)

```
Switch# show redundancy counters
Redundancy Facility OMs
               comm link up = 1
        comm link down down = 0

          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
        errored peer msg rx = 0

                 buffers tx = 656
     tx buffers unavailable = 0
                 buffers rx = 1302
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0
```

Table A-30 show redundancy counters Field Descriptions

Field	Description
comm link up	Shows how many communications links are up.
comm link down down	Shows how many communications links are down.
invalid client tx	Shows the number of invalid client transmissions.
null tx by client	Shows the number of null transmissions by the client.
tx failures	Shows the number of transmission failures.
tx msg length invalid	Shows the number of transmission messages with invalid lengths.
client not rxing msgs	Shows that the client is not receiving event messages.
rx peer msg routing errors	Shows errors occurring in the RF application. This usually indicates a software problem.
null peer msg rx	Shows that the interprocess communication (IPC) has sent an empty message to the RF application. This usually indicates a software problem.
errored peer msg rx	Shows an IPC error when an RF message was received. This usually indicates a software problem.
buffers tx	Shows the number of internal buffers acquired for sending RF messages.
tx buffers unavailable	Shows the number of times internal buffers for sending RF messages were not available due to the high volume of messages being sent. This usually indicates a software problem.
buffers rx	Shows the number of buffers released back to the internal buffer pool.
buffer release errors	Shows errors in releasing internal buffers.
duplicate client registers	Shows that an application has been registered with the RF more than once. This usually indicates a software problem.
failed to register client	Shows that the system was unable to register an RF client application due to low memory or a software problem.
Invalid client syncs	Shows an internal software problem in the RF.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy history

To display internal redundancy software history, use the **show redundancy history** command.

show redundancy history

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the internal redundancy software history log, which can be used to debug redundancy software.

Examples

The following example shows how to display the internal redundancy software history log, which can be useful for debugging redundancy software. (See Table A-31 for field descriptions.)

```
Switch# show redundancy history
Redundancy Facility Event Log:
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(19) seq=9999
00:00:16 client added: CPU Redundancy(17) seq=40
00:00:16 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:16 RF_PROG_INITIALIZATION(0) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_INITIALIZATION(0) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_INITIALIZATION(0) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:16 RF_STATUS_PEER_PRESENCE(12) op=0
00:00:16 RF_EVENT_GO_ACTIVE(28) op=0
00:00:16 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
00:00:16 RF_STATUS_SPLIT_ENABLE(15) CPU Redundancy(17) op=0
00:00:16 RF_PROG_ACTIVE_FAST(6) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_FAST(6) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_FAST(6) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_DRAIN(7) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_DRAIN(7) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_DRAIN(7) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE_PRECONFIG(11) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE_POSTCONFIG(12) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) RF_INTERNAL_MSG(0) op=0 rc=11
```

```
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE(13) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE(10) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE(10) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE(10) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 client added: OIR Client(6) seq=16
00:00:19 RF_STATUS_PEER_PRESENCE(12) op=0
00:00:36 Configuration parsing complete
00:00:36 System initialization complete
```

Table A-31 show redundancy history Field Descriptions

Field	Description
client added	Shows the RF subsystem client added.
*my state = INITIALIZATION	Shows that the CPU switch module has been initialized.
*peer state = DISABLED	Shows that the peer (or standby) CPU switch module is disabled.
Configuration parsing complete	Shows that the configuration has been read either from NVRAM or, on a switchover, from the stored running-config file.
System initialization complete	Shows that the system initialization is complete.

Related Commands

Command	Description
clear redundancy	Clears the redundancy history buffer in processor memory.
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy running-config-file

To display the running configuration on the standby CPU switch module, use the **show redundancy running-config-file** command.

show redundancy running-config-file

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command is only available on the standby CPU switch module. It shows the stored running-config file that has been synchronized from the active CPU switch module, which will be applied as the system configuration during the next standby to active transition.

If auto-synchronization is disabled for the running-config-file on the active CPU switch module, or if the IPC (interprocessor communications) is down, this command displays the message `running-config-file is not currently valid` and does not show the running-config-file.

Note While the standby CPU switch module remains in the hot-standby state, the running configuration, as shown by the **show running-config** command, is not expected to match the synchronized running-config file. Instead, it contains mostly default configuration values.

Examples

The following example displays the running-config file on the standby CPU switch module.

```
sby-Switch# show redundancy running-config-file
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
boot system flash bootflash:ons15530-i-mz
boot bootldr slot0:ons15530-i-mz

<Information deleted>
```

Table A-32 show redundancy running-config-file Field Descriptions

Field	Description
version	Shows the software version.
no service pad	Shows service pad configuration. In the output example, "no" indicates that incoming and outgoing packet assembler/disassembler (PAD) connections are not accepted.
service timestamps	Shows that logging appears with timestamps.
no service password-encryption	Shows that password encryption has been disabled.
hostname	Shows the system name.
boot system flash	Shows the boot system flash version.
boot bootldr	Shows the bootldr version.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

show redundancy states

To display internal redundancy software state information, use the **show redundancy states** command.

show redundancy states

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display internal redundancy software state information, which may be used to debug redundancy software.

Examples

The following example shows how to display internal redundancy software state information. (See Table A-33 for field descriptions.)

```
Switch> show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
        Unit ID = 6

     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 5
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 5000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 10
           RF debug mask = 0x0
```

Table A-33 show redundancy states Field Descriptions

Field	Description
my state	Shows the state of the active CPU switch module.
peer state	Shows the state of the peer (or standby) CPU switch module.

Table A-33 show redundancy states Field Descriptions (continued)

Field	Description
Mode	Shows either simplex (single CPU switch module) or duplex (two CPU switch modules) mode.
Unit	Shows either primary (or active) CPU switch module or peer (or standby) CPU switch module.
Unit ID	Shows the unit ID of the CPU switch module.
Split Mode	Indicates whether split mode is enabled or disabled.
Manual Swact	Indicates whether manual switchovers have been enabled without the force option.
Reason	Shows why manual switchovers have been disabled. Valid reasons are: • Simplex mode • Invalid peer state • Split mode • Progression in progress • Unidentified platform-specific reason
Communications	Indicates whether communications are up or down between the two CPU switch modules.
Reason	Shows why communications are down, either because the system is in simplex mode or due to a failure.
client count	Shows the number of redundancy subsystems that are registered as RF clients.
client_notification_TMR	Shows, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.
keep_alive TMR	Shows, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby CPU switch module.
keep_alive count	Shows the number of keep-alive messages sent without receiving a response from the standby CPU switch module.
keep_alive threshold	Shows the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).
RF debug mask	Shows an internal mask used by the RF to keep track of which debug modes are on.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant standby CPU switch module.
redundancy reload shelf	Reloads both redundant CPU switch modules in the shelf.

Command	Description
redundancy switch-activity	Manually switches activity from the active CPU switch module to the current standby CPU switch module.
show redundancy	Displays CPU switch module redundancy status and configuration information.

standby privilege-mode enable

To enable access to privileged EXEC mode from the standby CPU switch module CLI, use the **standby privilege-mode enable** command. To revert to the default state, use the **no** form of the command.

standby privilege-mode enable

no standby privilege-mode enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command must be entered on the active CPU switch module CLI before you can access privileged EXEC mode on the standby CPU switch module CLI.

Examples

The following example shows how to enable access to privileged EXEC mode on the standby CPU switch processor module.

```
Switch(config-red)# standby privilege-mode enable
```

Related Commands

Command	Description
show redundancy	Displays CPU switch module redundancy status and configuration information.

SNMP Commands

This section contains the Cisco ONS 15530-specific SNMP commands. For the complete list of SNMP commands supported on the Cisco ONS 15530, and their descriptions, refer to *Cisco IOS Configuration Fundamentals Command Reference* publication.

snmp-server enable traps aps

To enable SNMP trap notifications for APS activity, use the **snmp-server enable traps aps** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps aps

no snmp-server enable traps aps

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the APS MIB (CISCO-APS-MIB).

The **snmp-server enable traps aps** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for APS activity, the **snmp-server enable traps aps** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps aps
```

Related Commands

Command	Description
associate interface	Specifies interfaces to be associated and enters APS configuration mode.
show aps	Displays APS configuration information and status.
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps cdl

To enable SNMP trap notifications defined in CISCO-CDL-MIB, use the **snmp-server enable traps cdl** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

no snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

Syntax Description

all	Enables trap notifications on all in-band message channel capable interfaces.
terminating-interfaces	Enables trap notifications only on terminating interfaces for in-band message channel traffic.
soak-interval	Interval after which trap notifications are sent.
set-soak-interval	Time interval in milliseconds before sending defect indication trap notifications when a defect is set. The range is 100 to 60,000.
clear-soak-interval	Time interval in milliseconds before sending defect indication trap notifications when a defect is cleared. The range is 100 to 60,000.

Defaults

Disabled

Set interval: 2500 milliseconds

Clear interval: 10,000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the in-band message channel MIB (CISCO-CDL-MIB). SNMP trap notifications are sent when an in-band message channel connection is created, modified, or deleted.

The soak interval prevents the system from being flooded with set and clear notifications for defect indications. The default values for the soak interval are adequate for most network topologies.

The **snmp-server enable traps cdl** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps cdl** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps optical monitor min-severity

To enable SNMP trap notifications defined in optical monitor MIB with the minimum severity threshold, use the **snmp-server enable traps optical monitor min-severity** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps optical monitor min-severity {**critical** | **major** | **minor** | **not-alarmed**}

no snmp-server enable traps optical monitor min-severity {**critical** | **major** | **minor** | **not-alarmed**}

Syntax Description

critical	Enables trap notifications for critical optical monitor alarms.
major	Enables trap notifications for major optical monitor alarms.
minor	Enables trap notifications for minor optical monitor alarms.
not-alarmed	Enables trap notifications for optical monitor events.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the optical monitor MIB (CISCO-OPTICAL-MONITOR-MIB).

The **snmp-server enable traps optical monitor min-severity** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps optical monitor min-severity** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for major and critical optical monitor trap activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps optical monitor min-severity major.
```

Related Commands

Command	Description
patch	Configures patch connections.
show patch	Displays patch connection information.

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps oscp

To enable SNMP trap notifications for OSCP activity, use the **snmp-server enable traps oscp** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps oscp

no snmp-server enable traps oscp

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the OSCP MIB (CISCO-OSCP-MIB).

The **snmp-server enable traps oscp** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for OSCP activity, the **snmp-server enable traps oscp** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for OSCP activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps oscp
```

Related Commands

Command	Description
show oscp info	Displays OSCP configuration information.
show oscp neighbor	Displays OSCP neighbor information.
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps rf

To enable SNMP trap notification for CPU switch module redundancy activity, use the **snmp-server enable traps rf** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps rf

no snmp-server enable traps rf

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the Redundancy Facility MIB (CISCO-RF-MIB).

The **snmp-server enable traps patch** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps patch** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for CPU switch module redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
show redundancy	Displays redundancy configuration information and status.
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps threshold min-severity

To enable SNMP trap notifications for alarm thresholds, use the **snmp-server enable traps threshold min-severity** command. To disable this feature, use the **no** form of this command.

snmp-server enable traps threshold min-severity {**degrade** | **failure**}

no snmp-server enable traps threshold min-severity

Syntax Description

degrade	Specifies signal degrade as the minimum severity for SNMP trap notifications.
failure	Specifies signal failure as the minimum severity for SNMP trap notifications.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the alarm threshold MIB (CISCO-IF-THRESHOLD-MIB).

The **snmp-server enable traps threshold min-severity** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for alarm threshold activity, the **snmp-server enable traps threshold min-severity** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for alarm threshold activity and set the minimum severity to failure.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps threshold min-severity failure
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
show threshold-list	Displays the contents of a threshold list.

Command	Description
snmp-server host	Specifies the recipient for SNMP notification messages.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.

snmp-server enable traps topology

To enable SNMP trap notifications for the network topology activity, use the **snmp-server enable traps topology** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps topology [**throttle-interval** *seconds*]

no snmp-server enable traps topology [**throttle-interval** *seconds*]

Syntax Description

throttle-interval *seconds*	Specifies the number of seconds for the throttle timer interval. Valid values are 5 through 3600 seconds. If this keyword is omitted, the command defaults to 60 seconds at bootup time, or to the previous value configured.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the physical topology MIB (PTOPO-MIB).

The network topology trap throttle timer prevents the system from flooding the network with messages. We recommend a 60-second interval value.

The **snmp-server enable traps topology** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for physical topology activity, the **snmp-server enable traps topology** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to 30 seconds.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology throttle-interval 30
```

The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to the default value.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.
show topology	Displays global physical topology configuration.
topology neighbor cdp	Enables CDP on the interface.

snmp-server host

To specify the recipient for SNMP notification messages, use the **snmp-server host** command. To remove the specified host, use the **no** form of the command.

snmp-server host *host-addr* [**traps** | **informs**] [**version** [**1** | **2c** | **3** {**auth** | **noauth**}]]
community-string [**udp-port** *port*] [*notification-type*]

no snmp-server host *host-addr* {**traps** | **informs**}

Syntax Description

host-addr	Specifies the name or IP address of the targeted recipient host.
traps	Sends SNMP trap notifications to this host. This is the default. (Optional)
informs	Sends SNMP inform notifications to this host. (Optional)
version	Specifies the version of the SNMP used to send the traps. (Optional) Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified: • **1** —SNMPv1. This option is not available with informs. • **2c** —SNMPv2C. • **3** —SNMPv3. The following three optional keywords can follow the version 3 keyword: – **auth**—Enables MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) packet authentication. – **noauth**—Gives the noAuthNoPriv security level. This is the default if no keyword is specified.
community-string	Specifies the password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

udp-port *port*	Specifies the UDP port of the host to use. The range is 0 to 65535. The default is 162. (Optional)
notification-type	Specifies the type of notification to be sent to the host. (Optional) If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: • **alarms**—Sends alarm state change notifications (CISCO-ENTITY-ALARM-MIB). • **aps**—Sends APS MIB (CISCO-APS-MIB) modification notifications. • **bgp**—Sends BGP (Border Gateway Protocol) state change notifications. • **cdl**—Sends in-band message channel MIB (CISCO-CDL-MIB) modification notifications. • **config**—Sends configuration notifications. • **entity**—Sends entity MIB (ENTITY-MIB) modification notifications. • **fru-ctrl**—Sends entity FRU (field replaceable unit) control MIB (CISCO-ENTITY-FRU-CONTROL-MIB) modification notifications. • **optical power**—Sends optical power modification notifications. • **oscp**—Sends OSCP MIB (CISCO-OSCP-MIB) modification notifications. • **patch**—Sends optical patch MIB (CISCO-OPTICIAL-PATCH-MIB) modification notifications. • **rf**—Sends redundancy facility MIB (CISCO-RF-MIB) modification notifications. • **snmp**—Sends SNMP notifications (as defined in RFC 1157). • **syslog**—Sends error message notifications (CISCO-SYSLOG-MIB). Specify the level of messages to be sent with the logging history level command. • **threshold**—Sends interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) modification notifications. • **topology**—Sends physical topology MIB (PTOPO-MIB) modification notifications.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the system to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host** command to enable informs for a host and then enter another **snmp-server host** command to enable informs for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enabl**e command. Certain notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

Examples

The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server host node1 traps
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
show snmp	Displays the status of SNMP communications.
snmp-server enable traps aps	Enables SNMP trap notification for APS activity.
snmp-server enable traps cdl	Enables SNMP trap notification for in-band message channel activity.

Command	Description
snmp-server enable traps optical monitor min-severity	Enables SNMP trap notifications for OSCP activity.
snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.
snmp-server enable traps rf	Enables SNMP trap notifications for redundancy facility activity.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
snmp-server enable traps topology	Enables SNMP trap notifications for physical topology activity.

System Management Commands

Use the following commands to manage your Cisco ONS 15530.

clear facility-alarm

To clear the external indications for the facility alarms, use the **clear facility-alarm** command.

clear facility-alarm [**critical** | **major** | **minor**]

Syntax Description

critical	Specifies that all external critical alarm indications be cleared.
major	Specifies that all external major alarm indications be cleared.
minor	Specifies that all external minor alarm indications be cleared.

Defaults

Clears all external alarm indications and LEDs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to perform a one-time clear of the specified LEDS and external audible and visual alarm relays.

The facility alarm conditions and alarm threshold error conditions are still posted in the processor memory and can be seen by using the **show facility-alarm status** command. You can clear the alarm threshold error conditions in memory by disabling protocol monitoring using the **no monitor enable** command. Online removal of a component or disabling an interface with the **shutdown** command also clears an alarm from processor memory.

Examples

The following examples shows how to clear critical external facility alarm indications.

```
Switch# clear facility-alarm critical
```

Related Commands

Command	Description
monitor enable	Enables signal monitoring for certain protocol encapsulations.
show facility-alarm status	Shows the facility alarm status information.
shutdown	Disables an interface.

reload

To reload the active CPU switch module, use the **reload** command.

reload [*text* | **in** [*hh***:**]*mm* [*text*] | **at** *hh***:***mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description

text	Specifies a reason for reloading the active CPU switch module (maximum of 255 characters).
in [*hh*:]*mm*	Schedules a reload of the software to occur in the specified hours and minutes. The reload must occur within approximately 24 days.
at *hh:mm*	**Note** The **at** keyword can only be used if the system clock has been set (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the system. Schedules a reload of the software to occur at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to occur at that specified time and date. If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must occur within approximately 24 days.
month	Specifies the name of the month the reload is to occur, with any number of characters in a unique string.
day	Specifies the number of the day the reload is to occur, in the range 1 to 31.
cancel	Cancels a scheduled reload.

Defaults

Immediate active CPU switch module reload

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command halts the active CPU switch module. If the CPU switch module is set to restart on error, it reboots itself.

Use this command after configuration information is entered into a file and saved to the startup configuration. You cannot reload from a virtual terminal if the CPU switch module is not set up for automatic booting. This prevents the CPU switch module from dropping to the ROM monitor and thereby taking the CPU switch module out of the remote user’s control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you enter **yes** in this situation, the CPU switch module goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must occur within approximately 24 days.

This command can be entered on either the active or standby CPU switch module console and only a reload of the CPU switch module on which the command was entered occurs.

When entered on the active CPU switch module, this command synchronizes the running-config to the standby CPU switch module just before the reload is executed, and causes a switchover to the standby CPU switch module only if the standby CPU switch module is in the hot-standby state.

By default the system is configured to reboot automatically, so the active CPU switch module reboots as the standby CPU switch module after the reload.

To display information about a scheduled reload, use the **show reload** command.

Examples

The following example shows how to reload the software on the CPU switch module.

```
Switch# reload
```

The following example reloads the software on the CPU switch module in 10 minutes.

```
Switch# reload in 10
Reload scheduled for 11:57:08 PDT Mon Feb 26 2001 (in 10 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example reloads the software on the CPU switch module at 1:00 p.m. today.

```
Switch# reload at 13:00
Reload scheduled for 13:00:00 PPDT Mon Feb 26 2001 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example reloads the software on the CPU switch module on 2/27 at 2:00 a.m.

```
Switch# reload at 02:00 feb 27
Reload scheduled for 02:00:00 PDT Tues Feb 26 2001 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example cancels a pending reload.

```
Switch# reload cancel
%Reload cancelled.
```

Related Commands

Command	Description
config-register	Changes the configuration register settings.
maintenance-mode	Enables or disables CPU switch module redundancy synchronization.
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both CPU switch modules in the shelf.
redundancy switch-activity	Manually switches activity from the active CPU switch module to the standby CPU switch module.
show reload	Displays reload status information.

reprogram

To upgrade the FPGA or functional image on a selected card from a flash file, use the **reprogram** privileged EXEC command.

reprogram *flash-file-name* {*slot* [*subcard*] | **rommon** | **sby-rommon**}

Syntax Description

flash-file-name	Specifies the name of the image to download, which can be in the CompactFlash Card or bootflash.
slot	Specifies the physical slot number of the controller you want to reprogram. The slot number ranges from 0 to 10.
subcard	Indicate a subcard in a slot for half-width modules or in a carrier motherboard. The subcard number ranges from 0 to 3.
rommon	Specify reprogramming the ROMMON (ROM monitor) image of the active CPU switch card.
sby-rommon	Specify reprogramming the ROMMON image of the standby CPU switch card.

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command the image to the controller you select. It also resets the selected controller, which causes active connections and configurations to be lost.

Caution Do not power-cycle the system during a reprogram operation because damage can occur to the controller you are reprogramming. If you power-cycle the system while reprogramming is in progress, you also might be unable to boot the system.

Examples

The following example shows how to reprogram the image on the ESCON multiplexing line card in slot 3.

```
Switch# reprogram bootflash:fi-ons15530-escon.A.2-36.exo 3
```

Related Commands

Command	Description
show hardware	Displays hardware information for the system.
show version	Display version information for the Cisco IOS system image and the ROMMON image.

show bootvar

To display boot and related environmental variables for both the active and standby CPU switch modules, use the **show bootvar** command.

show bootvar

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

This command shows boot and related information for the active and standby CPU switch modules.

Examples

The following example shows how to display boot information for the system. (See Table A-34 for field descriptions.)

```
Switch# show bootvar
BOOT variable = bootflash:<imagename>;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2

Standby auto-sync startup config mode is on

Standby auto-sync running config mode is on

Standby is up.
Standby BOOT variable = bootflash:<imagename>;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable =
Standby Configuration register is 0x2
```

Table A-34 show bootvar Field Descriptions

Field	Description
BOOT variable	Shows a list of bootable images on various devices.
CONFIG_FILE variable	Shows the configuration file used during system initialization.

Table A-34 show bootvar Field Descriptions (continued)

Field	Description
BOOTLDR variable	Shows the configuration file used during system initialization.
Configuration register	Shows the stored configuration information.
Standby auto-sync startup config mode	Indicates whether startup-config file autosynchronization is enabled or disabled on the standby CPU switch module.
Standby auto-sync running config mode	Indicates whether running-config file autosynchronization is enabled or disabled on the standby CPU switch module.
Standby	Indicates whether the standby CPU switch module is up or down.
Standby BOOT variable	Shows a list of bootable images on various devices for the standby CPU switch module.
Standby CONFIG_FILE variable	Shows the configuration file used during system initialization for the standby CPU switch module.
Standby BOOTLDR variable	Shows the configuration file used during system initialization for the standby CPU switch module.
Standby Configuration register	Shows the stored configuration information for the standby CPU switch module.

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby CPU switch module.
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby CPU switch module.

show ciscoview package

To display Embedded CiscoView package information, use the **show ciscoview package** command.

show ciscoview package

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display Embedded CiscoView package file information or to troubleshoot.

Examples

The following example shows how to display Embedded CiscoView package information. (See Table A-35 for field descriptions.)

```
Switch# show ciscoview package

File source:slot1:
CVFILE                          SIZE(in bytes)
------------------------------------------------
ONS15530-1.0.html                8861
ONS15530-1.0.sgz                 1183238
ONS15530-1.0_ace.html            3704
ONS15530-1.0_error.html          401
ONS15530-1.0_jks.jar             17003
ONS15530-1.0_nos.jar             17497
applet.html                      8861
cisco.x509                       529
identitydb.obj                   2523
```

Table A-35 show ciscoview package Field Descriptions

Field	Description
File source	Identifies the slot.
CVFILE	Identifies the Embedded CiscoView files in the package.
SIZE (in bytes)	Shows the file size in bytes.

Related Commands

Command	Description
show ciscoview version	Displays Embedded CiscoView version information.

show ciscoview version

To display Embedded CiscoView version information, use the **show ciscoview version** command.

show ciscoview version

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display Embedded CiscoView version information.

Examples

The following example shows how to display Embedded CiscoView version information. (See Table A-36 for field descriptions.)

```
Switch# show ciscoview version

Engine Version: 5.3 ADP Device: ONS15530 ADP Version: 1.0 ADK: 39
```

Table A-36 show ciscoview version Field Descriptions

Field	Description
Engine Version	Identifies the Embedded CiscoView version.
ADP Device	Identifies the ADP (Autonomous Device Package) device.
ADP Version	Identifies the ADP version.

Related Commands

Command	Description
show ciscoview package	Displays Embedded CiscoView package information.

show facility-alarm status

To display the facility alarm status, use the **show facility-alarm status** command.

show facility-alarm status [**critical** | **info** | **major** | **minor**]

Syntax Description

critical	Shows the status information for critical facility alarms.
info	Shows the status information for information facility alarms.
major	Shows the status information for major facility alarms.
minor	Shows the status information for minor facility alarms.

Defaults

Displays all facility alarm status information. This information includes external alarms and protocol monitoring alarms.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the facility alarm and alarm threshold error status information.

Examples

The following example shows how to display the facility alarm status information. (See Table A-37 for field descriptions.)

```
Switch# show facility-alarm status
System Totals Critical: 1  Major: 10 Minor: 0
Source: Wave3/0         Severity: MAJOR    Description: 0    Loss of Lock event
Source: Wave3/0         Severity: MAJOR    Description: 1    Loss of Signal event
Source: Tran3/0/0       Severity: MAJOR    Description: 0    Loss of Lock event
Source: Tran3/0/0       Severity: MAJOR    Description: 1    Loss of Signal event
Source: voaFI2/0/0.1    Severity: MAJOR    Description: Low alarm threshold exceeded for
optical power
Source: voaFI2/0/0.2    Severity: MAJOR    Description: Low alarm threshold exceeded for
optical power
Source: voaFI2/1/0.1    Severity: MAJOR    Description: Low alarm threshold exceeded for
optical power
Source: Wave3/0/0       Severity: MAJOR    Description: Low alarm threshold exceeded for
Receive Power (in dBm)
Source: Wave3/0/1       Severity: MAJOR    Description: High alarm threshold exceeded for
Receive Power (in dBm)
Source: voaIN7/1/0      Severity: MAJOR    Description: Low alarm threshold exceeded for
optical power
Source: voaFI9/1/0.1    Severity: CRITICAL Description: Low alarm threshold exceeded for
optical power
```

Table A-37 show facility-alarm status Field Descriptions

Field	Description
System Totals	Shows the number of alarms in the output display by severity.
Source:	Shows the system component that is the source of the alarm.
Severity:	Shows the severity of the alarm.
Description:	Shows a description of the alarm. If a number is present at the beginning of the description, it is the index of the alarm.

Related Commands

Command	Description
clear facility-alarm	Clears external facility alarm indications.
monitor enable	Enables signal monitoring for certain protocol encapsulations.

show hardware

To display hardware information, use the **show hardware** command.

show hardware [**detail** | **linecard** [*slot*]]

Syntax Description

detail	Shows detailed hardware information for the entire shelf.
linecard [*slot*]	Shows detailed hardware information for the motherboard or CPU switch module in a specific slot. The range is 0 to 11.

Defaults

Displays summary hardware information for the entire shelf.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display hardware information for debugging and tracking.

Examples

The following example shows how to display hardware information for the shelf. (See Table A-38 for field descriptions.)

```
Switch# show hardware
--------------------------------------------------------------------------------
Prototype Hampton Backplane named Switch, Date: 15:02:03 UTC Sun Jun 23 2002
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Back-Plane Information
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Model     Ver Serial No.   MAC-Address       MAC-Size RMA No RMACode MFG-Date
--------- --- ------------ ----------------- -------- ------ ------- -----------
Prototype 3.1 TBC05502106  00-01-64-47-2a-b0 16                      10/21/2001
--------------------------------------------------------------------------------
Slot Orderable Product No.     Part No.   Rev Serial No.   Mfg. Date  H/W Ver.
---- ------------------------- ---------- --- ------------ ---------- ----------
0/0  PROTO-HAMPTONS-MUX/DEMUX  73-7399-01 2   CAB0539KMOS  11/02/2001 1.0
0/1  PROTO-HAMPTONS-MUX/DEMUX  73-7399-01 2   CAB0539KM12  11/02/2001 1.0
2/*  PROTO-HAMPTON-OSCMB       73-6838-04 01  CAB0603MAJ1  01/24/2002 4.0
2/0  PROTO-HAMPTON-OSCDC       73-7238-03 03  CAB0602MA36  12/07/2001 3.1
2/1  PROTO-HAMPTON-OSCDC       73-7238-03 03  CAB0602MA3H  12/07/2001 3.1
3/*  PROTO-HAMPTON-ESCON       73-7710-03 01  CAB0602M9PV  04/08/2002 3.2
4/*  PROTO-HAMPTON-TRANSPONDER 73-7675-04 02  CAB0551LWU1  05/14/2002 4.5
5/*  PROTO-HAMPTON-CPU         73-6572-04 06  CAB0606MGME  02/12/2002 4.6
7/*  PROTO-HAMPTON-TRANSPONDER 73-7675-04 02  CAB0551LWU1  05/14/2002 4.5
8/*  PROTO-HAM-10GE-DWDM       73-7933-04 1   CAB0553M5V3  12/01/2001 4.8
```

```
9/*  PROTO-HAMPTON-ESCON       73-7710-03 01  CAB0609MTE2  03/15/2002 3.3
10/* PROTO-HAM-10GE-DWDM       73-6765-03 2   CAB0605MDCC  12/01/2001 4.8

Power Supply:
Slot Part No.         Rev  Serial No.  RMA No.     Hw Vrs  Power Consumption
---- ---------------- ---- ----------- ----------- ------- -----------------
Unable to read idprom for 0
Power Supply 0 :
                type      : 600W AC
                status    : OK
Power Supply 1 Not present
```

Table A-38 show hardware Field Descriptions

Field	Description
Slot	Shows the slot or slot and subcard position for the hardware component.
Controller Type	Shows the hardware component controller type.
Part No.	Shows the part number.
Rev	Shows the revision number.
Serial No.	Shows the serial number.
Mfg. Date	Shows the date the component was manufactured.
RMA No.	Shows the RMA number.
H/W Ver.	Shows the hardware version number.

The following example shows how to display detailed hardware information for a specific slot. (See Table A-39 for field descriptions.)

```
Switch# show hardware linecard 3
--------------------------------------------------------------------------------
Slot Number             : 3/*
Controller Type         : 0x1101
On-Board Description    : HAMPTON-ESCON
Orderable Product Number: PROTO-HAMPTON-ESCON
Board Part Number       : 73-7710-03
Board Revision          : 01
Serial Number           : CAB0602M9PV
Manufacturing Date      : 04/08/2002
Hardware Version        : 3.2
RMA Number              :
RMA Failure Code        :
Functional Image Version: 2.36 (dec), 2.24 (hex)
```

Table A-39 show hardware linecard Field Descriptions

Field	Description
Slot Number	Shows the slot or slot and subcard position for the hardware component.
Controller Type	Shows the hardware component controller type.
On-Board Description	Shows the description stored on the component.
Orderable Product Number	Shows the component product order number.
Board Part Number	Shows the part number.
Board Revision	Shows the revision number.

Table A-39 show hardware linecard Field Descriptions (continued)

Field	Description
Serial Number	Shows the serial number.
Manufacturing Date	Shows the date the component was manufactured.
Hardware Version	Shows the hardware version number.
RMA Number	Shows the RMA number.
RMA Failure Code	Shows the RMA failure code.
Functional Image Version	Shows the version of the component functional image.

show optical wavelength mapping

To display the mapping of Cisco ONS 15530 channels to ITU grid frequencies and wavelengths, use the **show optical wavelength mapping** command.

show optical wavelength mapping

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display how the Cisco ONS 15530 channels map to the ITU G.692 grid wavelengths. Channel 0 is the OSC. Channels 1 through 32 are the client data channels. The last two digits of the frequency correspond to the ITU number (for example, the frequency for channel 1 is 192.1 so the ITU grid number is 21).

The frequencies ending in 0 and 5 are missing from the output because they are used as buffers between the 4-channel bands.

Examples

The following example shows how to display wavelength mapping information for the system. (See Table A-40 for field descriptions.)

```
Switch# show optical wavelength mapping
           Frequency    Wavelength
Channel      (THz)        (nm)
-------    ---------    ----------
  0          191.9        1562.23
  1          192.1        1560.61
  2          192.2        1559.79
  3          192.3        1558.98
  4          192.4        1558.17
  5          192.6        1556.55
  6          192.7        1555.75
  7          192.8        1554.94
  8          192.9        1554.13
  9          193.1        1552.52
  10         193.2        1551.72
  11         193.3        1550.92
  12         193.4        1550.12
  13         193.6        1548.51
  14         193.7        1547.72
  15         193.8        1546.92
  16         193.9        1546.12
  17         194.1        1544.53
  18         194.2        1543.73
  19         194.3        1542.94
  20         194.4        1542.14
  21         194.6        1540.56
  22         194.7        1539.77
  23         194.8        1538.98
  24         194.9        1538.19
  25         195.1        1536.61
  26         195.2        1535.82
  27         195.3        1535.04
  28         195.4        1534.25
  29         195.6        1532.68
  30         195.7        1531.90
  31         195.8        1531.12
  32         195.9        1530.33
```

Table A-40 show optical wavelength mapping Field Descriptions

Field	Description
Channel	Identifies the channel.
Frequency (THz)	Shows the frequency for the channel in THz. The last two digits correspond to the ITU grid number.
Wavelength (nm)	Shows the wavelength for the channel in nm.

show temperature

To display shelf temperature information, use the **show temperature** command.

show temperature

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the current shelf temperature and the alarm threshold temperatures.

Examples

The following example shows how to display internal redundancy software state information. (See Table A-41 for field descriptions.)

```
Switch> show temperature
   Sensor              Temperature                 Thresholds
                      (degree C)    Minor      Major     Critcal   Low
--------------------  -----------  ------------------------------------
Sensor                    27          65         75         80       -15

   Sensor                     Alarms
                      Minor   Major   Critical
--------------------  ------------------------
Sensor                  0          0         0
```

Table A-41 show temperature Field Descriptions

Field	Description
Sensor	Shows the type of sensor.
Temperature (degree C)	Shows the current temperature in degrees Celsius.
Minor	Shows temperature threshold that generates a minor alarm.
Major	Shows temperature threshold that generates a major alarm.
Critical	Shows temperature threshold that generates a critical alarm.
Low	Shows temperature threshold that generates a low alarm.
Alarms	Shows the number of minor, major, and critical alarms on the inlet and outlet sensors.

Related Commands

Command	Description
show facility-alarm status	Shows the facility alarm status information.

show version

To display the system hardware configuration, software version, and names and sources of configuration files and boot images, use the **show version** command.

show version

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the system hardware configuration, software version, and names and sources of configuration files and boot images.

Note Always specify the complete software version number when reporting a possible software problem.

Examples

The following example shows how to display version information for the system. Table A-42 describes the output from the **show version** command.

```
Switch# show version

  Cisco Internetwork Operating System Software
  IOS (tm) ONS-15530 Software (manopt-M0-M), Experimental Version 12.1(20001031:221042)
[ffrazer-man_cosmos 252]
  Copyright (c) 1986-2001 by cisco Systems, Inc.
  Compiled Fri 23-Feb-01 15:23 by ffrazer
  Image text-base:0x60010950, data-base:0x604E8000

  ROM:System Bootstrap, Version 12.1(20001031:194138) [ffrazer-man_cosmos 233],
DEVELOPMENT SOFTWARE
  BOOTFLASH:ONS-15530 Software (hamopt-M0-M), Experimental Version 12.1(20001031:221042)
[ffrazer-man_cosmos 246]

  Switch uptime is 30 minutes
  System returned to ROM by power-on
  System image file is "tftp://171.69.1.129/ffrazer/manopt-m0-mz.010223.6"

  cisco  (QUEENS-CPU) processor with 98304K/32768K bytes of memory.
  R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

  Last reset from power-on
  2 Ethernet/IEEE 802.3 interface(s)
  509K bytes of non-volatile configuration memory.

  20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
  16384K bytes of Flash internal SIMM (Sector size 64K).
  Configuration register is 0x102
```

Table A-42 show version Field Descriptions

Field	Description
Software version	Shows the software version.
Compiled	Shows the date and time the software was compiled.
System Bootstrap, Version	Shows the system bootstrap version number.
BOOTFLASH, Version	Shows the bootflash version number.
Switch uptime	Shows the number of days, hours, minutes, and seconds the system has been up and running.
System returned to ROM by power-on	Shows how the system was last booted—as a result of a normal system startup or because of system error.
System image file	Shows the name and location of the system image file.
bytes of memory	Shows the amount of system memory.
Last reset from power-on	Shows how the system was last reset.
2 Ethernet/IEEE 802.3 interface(s)	Shows the number, type, and encapsulation of interfaces available.
non-volatile configuration memory	Shows the amount of nonvolatile configuration memory available.
Flash PCMCIA	Shows the amount of Flash memory and location of the card.

Table A-42 show version Field Descriptions (continued)

Field	Description
Flash internal SIMM	Shows the amount of Flash internal SIMM memory.
Configuration register	Shows the location of the configuration register.

traceroute

To trace the IP routes the packets actually take when traveling from the Cisco ONS 15530 NME (network management Ethernet) port to their destination, use the **traceroute** EXEC command.

EXEC Mode

traceroute *protocol destination*

Privileged EXEC Mode

traceroute [*protocol*] [*destination*]

Syntax Description

protocol	Protocols that can be used are **appletalk**, **clns**, **ip**, **ipx**, and **vines**.In privileged EXEC mode, the default protocol is assumed for the destination address format.
destination	Destination address or host name on the command line. In privileged EXEC mode, the default parameters for the appropriate protocol are assumed.

Defaults

The *protocol* argument is based on the format of the *destination* argument. For example, if the system finds a destination in IP format, the protocol defaults to **ip**.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by the system when a datagram exceeds its TTL (Time To Live) value. The **traceroute** command starts by sending probe datagrams with a TTL value of 1. This causes the first system to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A `time exceeded` error message indicates that an intermediate system detected and discarded the probe. A `destination unreachable` error message indicates that the destination node received and discarded the probe because it could not deliver the packet. If the timer goes off before a response comes in, **traceroute** prints an asterisk(*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, enter **^X**.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and switches, the IP **traceroute** command may behave in unexpected ways.

Not all destinations respond correctly to a probe message by sending back an `ICMP port unreachable` message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL is reached, may indicate this problem.

There is a known problem with the way some hosts handle an `ICMP TTL exceeded` message. Some hosts generate an ICMP message, but they reuse the TTL of the incoming packet. Because this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually, the TTL gets high enough that the ICMP message can get back. For example, if the host is 6 hops away, **traceroute** times out in responses 6 through 11.

Examples

The following example displays sample IP **traceroute** output in EXEC mode when a destination host name is specified. (See Table A-43 for field descriptions.)

```
Switch> traceroute ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
        1 DEBRIS.CISCO.COM (131.108.1.6) 1000 msec 8 msec 4 msec
        2 BARRNET-GW.CISCO.COM (131.108.16.2) 8 msec 8 msec 8 msec
        3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
        4 BB2.SU.BARRNET.NET (131.119.254.6) 8 msec 8 msec 8 msec
        5 SU.ARC.BARRNET.NET (131.119.3.8) 12 msec 12 msec 8 msec
        6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
        7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table A-43 traceroute command Field Descriptions

Field	Description
1	Indicates the sequence number of the system in the path to the host.
DEBRIS.CISCO.COM	Shows the host name of this system.
131.108.1.61	Shows the IP address of this system.
1000 msec 8 msec 4 msec	Shows the round-trip time for each of the three probes that are sent.

Table A-44 describes the characters that can appear in **traceroute** output.

Table A-44 IP Trace Text Characters

Character	Description
nn msec	Indicates for each node the round-trip time in milliseconds for the specified number of probes.
*	Indicates that the probe timed out.
?	Indicates an unknown packet type.
Q	Indicates a source quench.
P	Indicates that the protocol is unreachable.
N	Indicates that the network is unreachable.
U	Indicates that the port is unreachable.
H	Indicates that the host is unreachable.

The following example displays sample IP **traceroute** output in privileged EXEC mode when a destination IP address is specified. (SeeTable A-45 for prompt descriptions and Table A-43 for field descriptions.)

```
Switch# traceroute
Protocol [ip]:
Target IP address: 10.0.0.1
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.0.0.2 msec 0 msec 4 msec
  2 10.0.1.9 0 msec 0 msec 0 msec
  3 10.0.0.1 0 msec 0 msec 4 msec
```

Table A-45 traceroute Command Prompt Descriptions

Prompt	Description
Protocol [ip]:	Specifies the protocol. The default is IP.
Target IP address:	Specifies the host name or an IP address. There is no default.
Source address:	Specifies one of the interface addresses of the router to use as a source address for the probes. The system will normally pick what it feels is the best source address to use.
Numeric display [n]:	Specifies the **traceroute** display format. The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds [3]:	Specifies the number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count [3]:	Specifies the number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]:	Specifies the TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]:	Specifies the largest TTL value that can be used. The default is 30. The **traceroute** command terminates when the destination is reached or when this value is reached.

Table A-45 traceroute Command Prompt Descriptions (continued)

Prompt	Description
Port Number [33434]:	Specifies the destination port used by the UDP probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	Specifies the IP header options. You can specify any combination. The **traceroute** command issues prompts for the required fields. Note that trace will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options. The default is no header options. The options are: • Loose—Allows you to specify a list of nodes that must be traversed when going to the destination. • Strict—Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination. • Record—Allows you to specify the number of hops to leave room for. • Timestamp—Allows you to specify the number of time stamps to leave room for. • Verbose—If you select any of the above options, the verbose mode is automatically selected and the **traceroute** command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

Threshold Commands

Interface alarm thresholds provide a way to monitor the quality of the client signal. Use the following commands to configure and monitor interface alarm threshold operations.

aps trigger

To enable y-cable line card protection signal switchover when the alarm thresholds are exceeded, use the **aps trigger** command. To disable y-cable protection signal switchover, use the **no** form of this command.

aps trigger

no aps trigger

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Threshold configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command in a y-cable protection configuration to cause a signal switchover when the active signal error rates exceed the alarm thresholds. The signal switchover occurs only if the standby signal is acceptable.

Note The threshold list must be applied to both interfaces in the associated pair.

Examples

The following example shows how to configure an APS switchover trigger for an alarm threshold.

```
Switch(config)# threshold-list sonet-alarms
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 6
Switch(config-threshold)# aps trigger
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# redundancy
Switch(config-red)# associate group chicago
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps revertive
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 3/0/0
Switch(config-if)# encap sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
Switch(config-if)# exit
Switch(config)# interface transparent 4/0/0
Switch(config-if)# encap sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
```

Related Commands

Command	Description
monitor enable	Enables protocol performance monitoring.
show threshold-list	Displays the contents of a threshold list.
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list to an interface.
threshold-list	creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

description

To configure a alarm threshold description, use the **description** command. To remove a threshold description, use the **no** form of the command.

description *text*

no description

Syntax Description

text	Threshold description for the MIB.

Defaults

None

Command Modes

Threshold configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

First use the **threshold-list** command to enter threshold list configuration mode and create a threshold list. Then use the **threshold** command to specify a threshold to modify and enter threshold configuration mode. This description can be accessed and displayed by network management systems that support SNMP.

Examples

The following example shows how to create a description for a threshold in a threshold list named temp.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)# threshold name sonet-sdh section cv degrade
Switch(config-threshold)# description This threshold is for SONET and SDH BIP1 errors
```

Related Commands

Command	Description
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list with an interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

notification-throttle timer

To modify the alarm threshold notification throttle timer, use the **notification-throttle timer** command. To return the notification throttle timer interval to its default value, use the **no** form of the command.

notification-throttle timer *seconds*

no notification-throttle timer

Syntax Description

seconds	Specifies, in seconds, the interval in which no more than one threshold alarm notification can be generated. If more than one notification is generated during the hold-down period, the extra notifications are delayed. The range is 5 to 500 seconds.

Defaults

5 seconds

Command Modes

Threshold list configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to control the amount of alarm threshold notification activity that is generated on the system.

Examples

The following example shows how to set an alarm threshold list notification throttle timer to 10 seconds.

```
Switch# configure terminal
Switch(config)# threshold-list sonet-alarms
Switch(config-t-list)# notification-throttle timer 10
```

Related Commands

Command	Description
show threshold-list	Displays the contents of a threshold list.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.

show threshold-list

To display information about alarm threshold lists, use the **show threshold-list** command.

show threshold-list [*name*]

Syntax Description

name	Specifies the name of an alarm threshold list.

Defaults

Displays information about all threshold lists in the system.

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the threshold values configured for all alarm threshold lists or for a specific alarm threshold list.

Examples

The following example shows how to display information for alarm threshold list named sonet-counters. (See Table A-46 for field descriptions.)

```
Switch# show threshold-list

Threshold List Name: sonet-counters
   Notification throttle timer : 5 (in secs)
   Threshold name : sonet-sdh section cv         Severity : Degrade
      Value : 10e-9
      APS Trigger : Not set
      Description : SONET BIP1 counter
   Threshold name : sonet-sdh section cv         Severity : Failure
      Value : 10e-6
      APS Trigger : Set
      Description : SONET BIP1 counter
```

Table A-46 show threshold-list Field Descriptions

Field	Description
Threshold List Name	Shows the name of the threshold list.
Notification throttle timer	Shows, in seconds, the interval in which no more than one threshold alarm notification can be generated. If more than one notification is generated during the hold-down period, the extra notifications are delayed.

Table A-46 show threshold-list Field Descriptions (continued)

Field	Description
Threshold name	Shows the name of the threshold counter. See the **threshold** command for a list of threshold names.
Severity	Shows the threshold severity (Degrade or Failure).
Value	Shows the threshold rate value for the system to issue an alarm.
APS Trigger	Indicates whether the APS switchover trigger is set.
Description	Shows the description text for the counter.

Related Commands

Command	Description
aps trigger	Enables APS switchover trigger for threshold alarms.
description	Configures MIB description for threshold alarms.
notification-throttle timer	Modifies the alarms threshold notification throttle timer.
snmp-server enable traps threshold min-severity	Enables SNMP trap notification for threshold alarms.
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list to a transparent or wave interface.
threshold-list	Creates a list of thresholds.
value	Configures the value for threshold alarms.

threshold

To configure an alarm threshold in a threshold list, use the **threshold** command. To remove a threshold from a threshold list, use the **no** form of the command.

threshold name {**8b10b cvrd** | **cdl hec** | **sonet-sdh section cv** | **crc**} {**degrade** | **failure**} [**index** *value*]

no threshold name {**8b10b cvrd** | **cdl hec** | **sonet-sdh section cv** | **crc**} {**degrade** | **failure**} [**index** *value*]

Syntax Description

8b10b cvrd	Specifies the coding violation and running disparity counter. This counter is monitored for interfaces with the following encapsulation: • Gigabit Ethernet • ESCON • Fibre Channel • FICON
cdl hec	Specifies the in-band message channel HEC (header error control) error counter. This counter is monitored for wave interfaces that insert and delete in-band message channel headers.
crc	Specifies the cyclic redundancy error counter.
sonet-sdh section cv	Specifies the bit interleaved parity error. This counter is monitored for interfaces with either SONET or SDH encapsulation.
degrade	Specifies that a signal degrade threshold alarm is generated.
failure	Specifies that a signal failure threshold alarm is generated.
index *value*	Specifies a MIB index. The range is 0 to 63.

Defaults

None

Command Modes

Threshold-list configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

First use the **threshold-list** command to enter threshold-list configuration mode and create a threshold list. Then use the **threshold** command to enter threshold configuration mode for the specific threshold. In threshold configuration mode, you can modify the threshold attribute values.

Interfaces have no default alarm threshold values. When monitoring is enabled, alarm thresholds are only in effect when a threshold list is associated with the interface.

By default, the **threshold** command uses the next available threshold index number in the threshold list MIB. The **index** keyword and value allow you to explicitly assign an index for the threshold. This is particularly useful as index numbers become available when thresholds are deleted.

Examples

The following example shows how to configure an alarm threshold in a threshold list and enter threshold configuration mode.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)# threshold name 8b10b cvrd degrade
Switch(config-threshold)#
```

Related Commands

Command	Description
aps trigger	Enables APS switchover when the alarm threshold is crossed.
description	Specifies a threshold description for the SNMP MIB.
notification-throttle timer	Modifies the alarm threshold notification throttle timer.
show threshold-list	Displays the contents of a threshold list.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
threshold-group	Associates a threshold list to an interface.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.
value	Specifies the threshold value.

threshold-group

To associate a threshold list to a transparent or wave interface, use the **threshold-group** command. To remove a threshold list from an interface, use the **no** form of this command.

threshold-group *name*

no threshold-group *name*

Syntax Description

name	Specifies the name of a threshold list and associates it with a specified interface.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to associate a threshold list to a specified interface.

Even though a threshold list might contain the thresholds for all error counters, not all of these thresholds are applicable to the interface. Thresholds are applied to the interface based on the interface type (wave or transparent) and the encapsulation type of the transparent interface.

If the interface is not associated with any threshold list, the threshold counters that are monitored on that interface are set to their default values.

Note For y-cable protected transparent and wave interfaces, disable monitoring on the interface with the **no monitor** command before removing an alarm threshold. Use the **show aps** command to determine the protection configuration for the interface.

Examples

The following example shows how to associate a threshold list to a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# threshold-group temp
```

Related Commands

Command	Description
show threshold-list	Displays the contents of a threshold list.
threshold	Creates failure and degrade thresholds for different error counters that are monitored on the interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

threshold-list

To create a list of thresholds, or modify an existing threshold list, use the **threshold-list** command. To delete the threshold list, use the **no** form of this command.

threshold-list *name*

no threshold-list *name*

Syntax Description

name	Specifies the name of the threshold list to be created and associated with a specified interface.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to create a list, or modify an existing list, of signal degrade and signal failure alarm thresholds for monitored error counters. After entering the command, the CLI enters threshold configuration mode where you can specify the threshold list attributes or threshold counters to add or modify.

Before deleting a threshold list, remove it from all the interfaces that use it.

Examples

The following example shows how to create a threshold list called temp.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)#
```

Related Commands

Command	Description
aps trigger	Enables APS switchover when the alarm threshold is crossed.
description	Specifies a threshold description for the SNMP MIB.
notification-throttle timer	Modifies the alarm threshold notification throttle timer.
show threshold-list	Displays the contents of a threshold list.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
threshold	Creates failure and degrade thresholds for different error counters that are monitored on the interface.

Command	Description
threshold-group	Associates a threshold list to an interface.
value	Specifies the threshold value.

value

To configure the values of failure and degrade alarm threshold rates, use the **value** command. To remove an threshold rate, use the **no** form of the command.

value rate *value*

no value

Syntax Description

rate *value*	Enters the threshold value as 10^{-x}, where *value* is x in 10^{-x}. The range is 3 to 9.

Defaults

None

Command Modes

Threshold configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

First use the **threshold-list** command to enter threshold-list configuration mode and create a threshold list. Then use the **threshold** command to specify a threshold to modify and enter threshold configuration mode.

The degrade rate value for a threshold must always be less than the failure rate value. For example, if the failure rate for a threshold is 7, or 10^{-7}, then the degrade value must be 8 or 9.

Table A-47 lists the errors per second for the threshold rates for each of the protocol encapsulations.

Table A-47 Thresholds for Monitored Protocols on Transponder Line Cards (Errors Per Second)

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel[1]	ISC[2]
3	31,753	32,000	32,000	1,244,390	199,102	1,057,731	1,057,731	1,057,731
4	12,318	27,421	31,987	124,944	19,991	106,202	106,202	106,202
5	1518	56,54	17,296	12,499	2000	10,625	10,625	10,625
6	155	616	2394	1250	200	1062	1062	1062
7	15.5	62	248	125	20	106	106	106
8	1.55	6.2	24.8	12.5	2	10.6	10.6	10.6
9	0.155	0.62	2.48	1.25	0.2	1.06	1.06	1.06

[1] Only 1 Gbps rate is supported.

[2] Compatibility mode only.

Table A-48 lists the threshold error rates in errors per second for ESCON signals on ESCON multiplexing line cards.

Table A-48 Threshold Values for Monitored Rates on ESCON Aggregated Signals (Errors Per Second)

Rate	ESCON CRC	ESCON CVRD	10 Gigabit Ethernet CVRD	10 Gigabit Ethernet CDL HEC
3	19999	20000	12,443,900	6512
4	19999	20000	1,249,438	665
5	1999	2000	124,944	67
6	199	200	10,312	7
7	20	20	1031	0.7
8	2	2	103	0.07
9	0.2	0.2	10	0.007

Examples

The following example shows how to create thresholds within a threshold list (temp) with the SONET and SDH section code violation error threshold signal degrade rate of 9 and signal failure rate of 7.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)# threshold name sonet-sdh section cv degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# end
Switch#
```

Related Commands

Command	Description
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list with an interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

Topology Neighbor Commands

Use the following commands to configure and monitor network topology neighbors.

show topology

To display information about the global physical network topology configuration, use the **show topology** command.

show topology

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the global physical network topology configuration information.

Examples

The following example shows how to display the topology hold-time interval. (See Table A-49 for field descriptions.)

```
Switch# show topology
Global Physical Topology configuration:
  Maximum Hold Time = 300 secs
 Trap interval = 60 secs
```

Table A-49 show topology hold-time Field Descriptions

Field	Description
Maximum Hold Time	Shows the maximum number of seconds a dynamically generated topology entry will remain before it times out.
Trap interval	Shows the number of seconds for the topology SNMP trap notification throttle interval.

Related Commands

Command	Description
show topology neighbor	Displays network topology information.
snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
topology hold-time	Modifies the interval to hold a nonstatic topology node entry.

show topology neighbor

To display the network topology neighbors for the shelf, use the **show topology neighbor** command.

show topology neighbor [**detail**]

Syntax Description

detail	Shows the agent IP address and how the topology entry was created.

Defaults

Displays summary information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to display the network topology neighbors for the shelf.

Examples

The following example shows how to display network topology neighbor information for the shelf. (See Table A-50 for field descriptions.)

```
Switch# show topology neighbor
Physical Topology:

Local Port          Neighbor Node       Neighbor Port        Link Dirn
----------          -------------       -------------        ---------
Wdm0/0              ham2                Wdm0/1               Both
Wdm0/1              ham2                Wdm0/0               Both
```

Table A-50 show topology neighbor Field Descriptions

Field	Description
Local Port	Identifies the local port.
Neighbor Node	Identifies the neighbor node.
Neighbor Port	Identifies the port or wdm interface on the neighbor node.

The following example shows how to display detailed network topology neighbor information for the shelf. (See Table A-51 for field descriptions.)

```
Switch# show topology neighbor detail
Physical Topology:

Local Port: Wdm0/0
Neighbor Node          : ham2
Neighbor Port          : Wdm0/1
Neighbor Agent Address: 1.1.1.10
Neighbor Discovery     : Via CDP (Proxy Port: Wave2/1)
Link Direction         : Both

Local Port: Wdm0/1
Neighbor Node          : ham2
Neighbor Port          : Wdm0/0
Neighbor Agent Address: 172.20.42.27
Neighbor Discovery     : Via CDP (Proxy Port: Wave2/0)
Link Direction         : Both
```

Table A-51 show topology neighbor detail Field Descriptions

Field	Description
Local Port	Identifies the local port.
Neighbor Node	Identifies the neighbor node.
Neighbor Port	Identifies the port on the neighbor node.
Neighbor Agent Address	Identifies the IP address of the topology agent on the neighbor node.
Neighbor Discovery	Indicates how the topology neighbor was discovered, either automatically via CDP or manually via the CLI.

Related Commands

Command	Description
show topology	Displays global physical topology configuration.
snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor agent ip-address	Specifies the network management agent address on a remote node.
topology neighbor cdp	Enables CDP on wdm interfaces.
topology neighbor disable	Removes an interface from the network topology.
topology hold-time	Modifies the interval to hold a nonstatic topology node entry.

topology hold-time

To modify the interval to hold nonstatic topology node entries, use the **topology hold-time** command. To return the hold-time interval to its default value, use the **no** form of the command.

topology hold-time *seconds*

no topology hold-time

Syntax Description

seconds	Specifies the number of seconds. The range is 1 to 2147483647 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to modify the network topology hold-time timer interval. This timer helps avoid reconstructing a nonstatic topology entry when a node leaves the network for only a brief time.

Examples

The following example shows how to modify the network topology hold time.

```
Switch# configure terminal
Switch(config)# topology hold-time 60
```

Related Commands

Command	Description
show topology	Displays global physical topology configuration.
snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
topology neighbor cdp	Enables CDP on wdm interfaces.

topology neighbor

To manually add a static entry for a filterband, filtergroup, thru, OSC wave, oscfilter, transparent, or wdm interface to the network topology, use the **topology neighbor** command.

To remove the interface from the network topology, use the **no** form of the command or the **topology neighbor disable** command.

topology neighbor {**name** *node-name*| **ip-address** *ip-address* |
  mac-address *mac-address*} {**port name** *port-name* | **port ip-address** *port-ip-address* |
  port mac-address *port-mac-address*} **[transmit | receive]**

no topology neighbor

Syntax Description

name *node-name*	Specifies the name of the neighbor node.
ip-addess *ip-address*	Specifies the IP address of the neighbor node.
mac-address *mac-address*	Specifies the MAC address of the neighbor node.
port name *port-name*	Specifies the name of the port on the neighbor node.
port ip-address *port-ip-address*	Specifies the IP address of the port on the neighbor node.
port mac-address *port-mac-address*	Specifies the MAC address of the port on the neighbor node.
transmit	Indicates that the link to the neighbor is transmit only.
receive	Indicates that the link to the neighbor is receive only.

Defaults

CDP (Cisco Discovery Protocol) is enabled on wdm interfaces.

Both directions.

No topology is configured on transparent interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to manually add wdm, thru, oscfilter, OSC wave, filterband, filtergroup, and transparent interfaces to the network topology. You must also configure the network management agent IP address with the **topology neighbor agent ip-address** command. By default, CDP is enabled on all these interface types.

For transparent interfaces, you must use the **topology neighbor** command to add the interface to the network topology because the transparent interfaces do not support CDP. For wdm interfaces, use either the **topology neighbor** command or the **topology neighbor cdp** command to populate the network topology.

For y-cable protected configurations, add both associated transparent interfaces to the network topology.

You can also use the **topology neighbor disable** command to remove an interface from the network topology.

Use the direction option to distinguish between bidirectional link neighbors and unidirectional (transmit or receive) link neighbors.

Examples

The following example shows a configuration example of network topology neighbor for the shelf. This allows either 1 bidirectional neighbor or 2 unidirectional neighbors on 1 interface.(See Table A-50 for field descriptions.)

```
Switch(config)# interface transparent 8/0/0
Switch(config-if)# topology neighbor name edfa1 port name inport transmit
Switch(config-if)# topology neighbor name edfa2 port name outport receive
Switch(config-if)# topology neighbor agent ip-address 10.0.0.31 transmit
Switch(config-if)# topology neighbor agent ip-address 10.0.0.32 receive
Switch(config-if)# exit
Switch(config)# interface transparent 8/0/0
Switch(config-if)# topology neighbor name 15530-box2 port name wdm0/0
Switch(config-if)# topology neighbor agent ip-address 10.0.0.20
Switch(config-if)# end
Switch#
```

The following example shows how to connect an OADM module to an OADM module in another node.

```
Switch# configure terminal
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor name NodeA port name wdm0/0
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

The following example shows how to connect an OADM module to an interface on client equipment.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# topology neighbor name Router1 port name gigabitethernet2/1
Switch(config-if)# topology neighbor agent ip-address 10.2.2.2
```

Related Commands

Command	Description
show topology neighbor	Displays network topology information.
snmp-server enable traps topology	Enables SNMP trap notifications for the network topology.
topology neighbor agent ip-address	Specifies the network management agent IP address.
topology neighbor cdp	Enables CDP on wdm interfaces.
topology neighbor disable	Removes the interface from the network topology.

topology neighbor agent ip-address

To specify the network management agent address on a remote node, use the **topology neighbor agent ip-address** command. To remove the network management agent address from an interface, use the **no** form of the command.

topology neighbor agent ip-address *ip-address* [**transmit** | **receive**]

no topology neighbor agent ip-address *ip-address* [**transmit** | **receive**]

Syntax Description

ip-address	Specifies the IP address of the network management agent on the neighbor node or remote node. This address is usually the IP address configured on the NME interface on the neighbor node.
transmit	Indicates that the link to the neighbor is transmit only.
receive	Indicates that the link to the neighbor is receive only.

Defaults

Both directions

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command if you have configured a network topology manually with the **topology neighbor** command. Use this command on both wdm and transparent interfaces.

The network management agent IP address is usually the IP address of the NME on the node.

Note Do not use this command if you have enabled CDP on the interface with the **topology neighbor cdp** command.

Examples

The following example shows how to configure a network management agent on a wdm interface.

```
Switch# configure terminal
Switch(config)# interface wdm 0/2
Switch(config-if)# topology neighbor name NodeA port name wdm0/0
Switch(config-if)# topology neighbor agent ip-address 209.165.202.129
```

The following example shows how to configure a network management agent on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/00
Switch(config-if)# topology neighbor name Router2 port name gigabitethernet 2/2
Switch(config-if)# topology neighbor agent ip-address 209.165.202.130
```

The following example shows how to configure directional parameters for a network management agent on a remote transparent interface.

```
Switch(config)# interface transparent 8/0/0
Switch(config-if)# topology neighbor name edfa1 port name inport transmit
Switch(config-if)# topology neighbor name edfa2 port name outport receive
Switch(config-if)# topology neighbor agent ip-address 10.0.0.31 transmit
Switch(config-if)# topology neighbor agent ip-address 10.0.0.32 receive
Switch(config-if)# exit
```

Related Commandsv

Command	Description
show topology neighbor	Displays the topology configuration.
topology neighbor	Adds a static entry for an interface to the network topology.

topology neighbor cdp

To enable CDP topology discovery on a wdm interface, use the **topology neighbor cdp** command. To disable CDP topology discovery on the interface, use the **no** form of the command or the **topology neighbor disable** command.

topology neighbor cdp [**proxy** *interface*]

no topology neighbor cdp [**proxy** *interface*]

Syntax Description

proxy *interface*	Specifies the interface capable of learning the topology to use as a proxy for CDP. Only OSC wave interfaces and ethernetdcc interfaces can be used as proxy interfaces.

Defaults

Topology discovery enabled

The OSC wave interface patched to the oscfilter interface on the same OADM as the wdm interface is the default proxy interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

CDP dynamically adds wdm interfaces to and removes wdm interfaces from the network topology. For CDP discovery to function properly, the OSC or in-band message channel, and CDP must be present and configured on the system. Use the **proxy** option to specific either an OSC wave interface or an ethernetdcc interface on a 10-Gbps ITU trunk card or 10-GE uplink card. These types of interfaces are capable of learning the topology using CDP.

You can use the **topology neighbor** command to statically add a wdm interface to the network topology, but you must first disable CDP on the interface. To configure a transparent interface as part of the network topology, use the **topology neighbor** command.

Note To use the default proxy interface, you must correctly configure the patch connections between the OADM modules and the OSC modules using the **patch** command. Otherwise, CDP cannot locate the OSC wave interfaces that connect to the trunk fiber and discover the topology neighbors.

Examples

The following example shows how to enable CDP on a wdm interface.

```
Switch# configure terminal
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor cdp proxy wave 2/0
```

Related Commands

Command	Description
patch	Configures the patch connections between the OADM modules.
show topology neighbor	Displays the topology configuration.
snmp-server enable traps topology	Enables SNMP trap notifications for the network topology.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor disable	Removes the interface from the network topology.

topology neighbor disable

To remove an interface from the network topology, use the **topology neighbor disable** command.

topology neighbor disable

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
12.1(10)EV2	This command was introduced.

Usage Guidelines

Use this command to remove an interface from the network topology, whether it was added with the **topology neighbor** command or the **topology neighbor cdp** command.

Examples

The following example shows how to remove an interface from the network topology.

```
Switch# configure terminal
Switch(config)# interface wdm 0/2
Switch(config-if)# topology neighbor disable
```

Related Commands

Command	Description
show topology neighbor	Displays the system connections.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor cdp	Enables CDP on the interface.

INDEX